ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Τεχνοοικονομική μελέτη, σχεδιασμός και υλοποίηση δικτύου κορμού με δυνατότητα σύνδεσης ετερογενών κόμβων αισθητήρων για Internet of Things (IoT) εφαρμογές.

ΤΣΑΡΑ ΠΑΝΑΓΙΩΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
Επιβλέπων
Σταμούλης Γεώργιος

Λαμία, 2019

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Design and implementation of core network with heterogeneous sensor nodes for IoT applications

Tsara Panagiota

Master thesis

Supervisor
Stamoulis Georgios

Lamia, 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

Τεχνοοικονομική μελέτη, σχεδιασμός και υλοποίηση δικτύου κορμού με δυνατότητα σύνδεσης ετερογενών κόμβων αισθητήρων για Internet of Things (IoT) εφαρμογές.

ΤΣΑΡΑ ΠΑΝΑΓΙΩΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων
Σταμούλης Γεώργιος

Λαμία, 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η ΔΗΛΩΝ/-ΟΥΣΑ

Ημερομηνία

Υπογραφή

Τεχνοοικονομική μελέτη, σχεδιασμός και υλοποίηση δικτύου κορμού με δυνατότητα σύνδεσης ετερογενών κόμβων αισθητήρων για Internet of Things (IoT) εφαρμογές.

ΤΣΑΡΑ ΠΑΝΑΓΙΩΤΑ

Τριμελής Επιτροπή:

Σταμούλης Γεώργιος, Καθηγητής (επιβλέπων)

Κοζύρη Μαρία, Επίκουρη Καθηγήτρια

Δημητρίου Γεώργιος, Επίκουρος Καθηγητής

Επιστημονικός Σύμβουλος:

Ξενάκης Απόστολος, Πανεπιστημιακός Υπότροφος

ΠΕΡΙΛΗΨΗ

Στην πτυχιακή αυτή εργασία θα γίνει μία τεχνοοικονομική μελέτη και θα προταθεί ο σχεδιαμός ενός δικτύου κορμού ενός Smart Home με δυνατότητα σύνδεσης αισθητήρων για IoT εφαρμογές ελέγχου. Συγκεκριμένα θα υλοποιηθούν IoT σενάρια μέσω τεχνολογιών ελέγχου. Η εργασία θα αποτελείται από τα εξης παραδοτέα:

1) Τεχνοοικονομική μελέτη δικτύου

2) Σχεδιασμός του δικτύου (ποιές συσκευές θα συμμετέχουν και πως θα συνδέονται)

3) Διευθυνσιοδότηση και παραμετροποίηση των συσκευών (pc, laptops, servers, IoT sensor nodes, κ.α.) βάση του Ipv4 πρωτοκόλλου.

4) Αλγόριθμοι δρομολόγησης δεδομένων μεταξύ δικτύου κορμού και IoT δικτύου.

5) Ρύθμιση πολιτικών ασφάλειας και προστασίας δεδομένων

6) Παραμετροποίηση IoT sensor nodes για μέτρηση φυσικών μεγεθών. Τα εργαλεία που χρησιμοποιήθηκαν είναι το Cisco Packet Tracer 7.2 emulator, JavaScript and/or Python scripts για τον προγραμματισμό των IoT κόμβων/αισθητήρων.

ABSTRACT

The present Master Thesis presents a techno-economic study and proposes the design of a core network architecture of a Smart Home with heterogeneous sensor nodes for IoT applications. This project consists of the following deliverables:
1) Techno-economic study and implementation of the core network
2) Design of the network (which devices are used and how are they connected)
3) Addressing and configuration of all the devices of the network (pc, laptops, servers, IoT sensor nodes, etc.) based on the IPv4 protocol 4) Routing algorithms and protocols that are used between the core network and the IoT network.
5) Analysis and implementation of security policies and data protection regulating techniques used in the Smart Home network
6) Configuration of IoT sensor nodes.
The tools that have been used in this project are the Cisco Packet Tracer 7.2 emulator, JavaScript and/or Python scripts for the programming of the IoT sensor nodes.

ΕΥΧΑΡΙΣΤΗΡΙΟ ΣΗΜΕΙΩΜΑ

Τελειώνοντας τη διπλωματική μου εργασία, θα ήθελα να ευχαριστήσω ιδαίτερα την οικογένεια μου, που ήταν δίπλα μου με κάθε τρόπο βοηθώντας με είτε ψυχολογικά είτε οικονομικά κατά τη διάρκεια των σπουδών μου αλλά και της τελευταίας μου υποχρέωσης για την απόκτηση του μεταπτυχιακού μου από το Πανεπιστήμιο Θεσσαλίας. Το μεγαλύτερο ευχαριστώ όμως το χρωστάω στον αδερφό μου που με μύησε στην Επιστήμη των Υπολογιστών και μου μετέδωσε τις γνώσεις του.

Ένα μεγάλο ευχαριστώ οφείλω και στους φίλους και το φίλο μου για την υπομονή και βοήθεια τους κατά τη διάρκεια του μεταπτυχιακού μου.

Τέλος, ένα μεγάλο ευχαριστώ οφείλω στον επιβλέποντα καθηγητή μου κ. Γεώργιο Σταμούλη για την εμπιστοσύνη του στο πρόσωπο μου και στον μέντορά μου, κ. Απόστολο Ξενάκη για την υποστήριξη, την κατανόηση και τις συμβουλές του, την επιλογή του θέματος που μου ταίριαζε απόλυτα και μου άνοιξε τις πόρτες της επαγγελματικής μου εξέλιξης.

Table of Contents

Κεφάλαιο 1: Εισαγωγή

Αν και το νευρωνικό δίκτυο τον ειδοποίησε στην ώρα του, όπως κάθε μέρα, εν' τούτοις ένοιωθε πως καθυστέρησε με την δυσλειτουργία του ηλεκτρονικού θερμαντήρα νερού. Άγγιξε βιαστικά την παλάμη του, κάλεσε την υπηρεσία πάρκινγκ για άνοιγμα της πόρτας, ξεκίνημα του αυτοκινήτου με κατεύθυνση προς την πόρτα του. Εκτίμησε δεόντως την ταχύτητα βίο-αναγνώρισης με την ίριδα και χαμογέλασε όταν θυμήθηκε πως ελάχιστα χρόνια πριν, χρειαζόταν κάποιος να κάνει το ίδιο με δαχτυλικά αποτυπώματα και tap σε οθόνες. Μπαίνοντας στο αυτοκίνητο ξεκίνησε αυτόματα η ενημέρωση βάσει των προτιμήσεών του, ενώ ο εγκέφαλος του αυτοκινήτου, συνδεόταν στο δίκτυο ηλεκτρονικής κυκλοφορίας με κατεύθυνση την Εταιρεία. Επικοινώνησε ολογραφικά με το τμήμα του για τις προτεραιότητες της ημέρας, δίνοντας παράλληλα φωνητική εντολή στο σύστημα υπενθύμισης για τις απογευματινές του δραστηριότητες....[1]

Σενάριο επιστημονικής φαντασίας ή και όχι;

Μέσα στο εξόχως ενδιαφέρον και πάντοτε ανατρεπτικό επιστημονικό τοπίο, το τεχνολογικό μέλλον βάζει προκλήσεις στους επιστήμονες ώστε οι νέες ιδέες τους να συνδέονται άρρηκτα με την καινοτομία και τον νεωτερισμό. Υπάρχουν τάσεις της τεχνολογίας που πεθαίνουν πριν καλά-καλά γεννηθούν κι άλλες που καταλήγουν να είναι τόσο σημαντικές που αλλάζουν ουσιαστικά τον τρόπο που ζούμε. Έτοιμοι ή όχι, οι εταιρείες έχουν αρχίσει ήδη να κινούνται στην κατεύθυνση αυτού που ακούμε και διαβάζουμε όλο και πιο συχνά το τελευταίο διάστημα, το: **Internet of Things** (IoT) ή το **Διαδίκτυο των Πραγμάτων**.

Τι είναι το Internet of Things; Είναι ακριβώς όπως ακούγεται: Πράγματα που έχουν Ίντερνετ. Ποιά ακριβώς πράγματα μπορεί να είναι αυτά αναρωτιέστε; Η απάντηση είναι οτιδήποτε, από ένα διασυνδεδεμένο στο Διαδίκτυο ψυγείο, ένα πλυντήριο, ο συναγερμός μέχρι και ολόκληρο το ασύρματα συνδεδεμένο σπίτι σου ή μια «έξυπνη πόλη». Το μέλλον της μετάβασης από δίκτυα υπολογιστών σε δίκτυα διασυνδεδεμένων αντικειμένων και προϊόντων γίνεται ήδη παρόν και θα κάνει τη καθημερινή ζωή όλων πιο εύκολη. Δια στόματος Kevin Ashton, επινοητή του όρου Internet of Things το 1999, «Οι άνθρωποι έχουν φυσική υπόσταση, το ίδιο και το περιβάλλον στο οποίο ζούμε. Δεν μπορείς να φας bits, ή να τα κάψεις για να σε κρατήσουν ζεστό, κι όμως, το σήμερα της κοινωνίας, της οικονομίας και της επιβίωσης δεν βασίζεται σε ιδέες ή πληροφορίες αλλά βασίζεται σε πράγματα. Ο στόχος ήταν να δώσουμε τη δύναμη στους υπολογιστές να μπορούν να συλλέγουν τις πληροφορίες με δικά τους μέσα, ώστε να μπορούν να δουν, να ακούσουν, να μυρίσουν τον κόσμο οι ίδιοι όπως θα έκανε ένας άνθρωπος αλλά χωρίς τη χείρα βοηθείας του. Η τεχνολογία ραδιοσυχνικής αναγνώρισης (RFID) και η τεχνολογία των αισθητήρων κατέστησε ικανούς τους υπολογιστές να παρακολουθούν, να αναγνωρίζουν και να καταλαβαίνουν τον κόσμο έξω από τα όρια της ανθρώπινης ικανότητας.» [22]

Το χθές και το σήμερα του IoT

Η αρχή του IoT έγινε με το Ασύρματο Διαδίκτυο, τις συσκευές με Wi-Fi δυνατότητες και ενσωματωμένους αισθητήρες όπως τα smart phones, φτάνοντας στη σημερινή εκδοχή και λογική του IoT όπου οι συσκευές συνδέονται με το Διαδίκτυο αλλά και μεταξύ τους. Ας τα δούμε λοιπόν από την αρχή.

Αν και η πρώτη ιδέα του IoT έκανε την εμφάνιση της σχεδόν πριν δυο δεκαετίες, οι τεχνολογίες οι οποίες έθεσαν τα θεμέλια για το σχηματισμό του και την υποστήριξή του υπάρχουν στο προσκήνιο εδώ και πολλά χρόνια. Αρχικά, όπως υποδηλώνει και το όνομα του, μια από τις πιο βασικές τεχνολογίες είναι το ίδιο το Internet, το οποίο έχει τις ρίζες του στο ερευνητικό σχέδιο του ARPANET που ξεκίνησε το 1969 χρηματοδοτούμενο από το Γραφείο Ερευνών Αμύνης των Ηνωμένων Πολιτειών, με σκοπό να δοθεί για χρήση στα πανεπιστήμια και σε εργαστήρια ερευνών στις Η.Π.Α. Σήμερα το Internet είναι ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών σε ένα κοινό δίκτυο, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων Internet εξυπηρετώντας καθημερινά εκατομμύρια χρήστες ανά τον κόσμο. [24]

Ακόμη μια θεμελιώδης τεχνολογία για το IoT είναι τα Ενσωματωμένα Συστήματα Υπολογιστών (Embedded Systems). Αυτός ο όρος χρησιμοποιήθηκε αρχικά το 1974 και περιγράφει εξειδικευμένα συστήματα υπολογιστών, τα οποία είναι αφοσιωμένα στην εκτέλεση μιας συγκεκριμένης λειτουργίας και είναι ενσωματωμένα σε ένα μεγαλύτερο σύστημα ή προϊόν. Ένα ενσωματωμένο σύστημα σχεδιάζεται για μία μόνο λειτουργία και την εκτελεί αδιαλείπτως. Η σημαντική πρόοδος στους επεξεργαστές τα έκανε προσιτά στο καταναλωτικό κοινό, με γνωστό παράδειγμα τις πλακέτες αυτόνομων μικροελεγκτών Raspberry-Pi, Arduino, Lego Mindstorms.

Στις αρχές του 1990, ο Mark Weiser έγινε γνωστός ως ο πατέρας της Πανταχού Παρούσας Υπολογιστικής ή αλλιώς Διάχυτης Υπολογιστικής (Ubiquitous Computing), της οποίας η κεντρική ιδέα είναι οι υπολογιστές να είναι πάντα και παντού ταυτοχρόνως παρόντες αλλά και αόρατοι. Αόρατοι, σημαίνει ότι οι υπολογιστές πρέπει να είναι τόσο αποτελεσματικά και αρμονικά ενσωματωμένοι με το φυσικό περιβάλλον, ώστε να τους χρησιμοποιούμε χωρίς ουσιαστικά να το αντιλαμβανόμαστε. Η ραχοκοκαλιά του Ubiquitous Computing έγκειται στον συνδυασμό των πλεονεκτημάτων των Ενσωματωμένων Συστημάτων των προηγούμενων ετών και της ανάπτυξης ενός πανταχού παρόντος δικτύου, κλίμακας εκατοντάδων υπολογιστών ανά δωμάτιο. Η τεχνολογία υποχωρεί στο παρασκήνιο και οι διαδικασίες υπολογιστικής πραγματοποιούνται οπουδήποτε και οποτεδήποτε. Η Διάχυτη Υπολογιστική είναι κατά προσέγγιση το αντίθετο της εικονικής πραγματικότητας, διότι αναγκάζει τους υπολογιστές να συμβιώσουν έξω στον κόσμο με τους ανθρώπους και όχι ο άνθρωπος να ζει μέσα σε έναν κόσμο δημιουργημένο από υπολογιστές.

Μέχρι τα μέσα του 1990, οι κόμβοι αισθητήρων άρχισαν να αναπτύσσονται ενώ παράλληλα άλλες τεχνολογίες, όπως οι ασύρματες επικοινωνίες και τα ψηφιακά ηλεκτρονικά άρχισαν να σημειώνουν σημαντικές εξελίξεις.[26] Οι αισθητήρες είναι μικροσκοπικές αυτόνομες μονάδες οι οποίες «αισθάνονται» φυσικά μεγέθη όπως η θερμοκρασία, η πίεση, η υγρασία, η κίνηση, ο ήχος κ.α. και μεταδίδουν την επεξεργασμένη ή και μη μέτρησή τους μέσω ενός δικτύου. Συγκεκριμένα, τα «πράγματα» στο IoT (Διαδίκτυο των Πραγμάτων) μοιράζονται κάποια από τα χαρακτηριστικά των κόμβων αισθητήρων. [28]

Σύνθετες σκέψεις για το IoT

Οι εκτιμήσεις της τεχνολογικής βιομηχανίας για το IoT δείχνουν πως αυτή η τάση θα κυριαρχήσει. Η εταιρία ερευνών αγοράς Gartner εκτιμά ότι μέχρι το 2020 περισσότερα από 250 εκατομμύρια αυτοκίνητα θα είναι συνδεδεμένα στο Ίντερνετ παρέχοντας έξυπνες λειτουργίες και σαφώς υπηρεσίες αυτόνομης οδήγησης. Η εταιρία τεχνολογικών μελετών IHS επίσης προβλέπει ότι μέχρι το 2020 θα υπάρχουν περισσότερες από 75 δισεκατομμύρια συσκευές συνδεδεμένες

στο Ίντερνετ. Τίποτα από αυτά δεν θα ήταν εφικτό χωρίς τα τεράστια άλματα που συντελούνται στον τομέα της πληροφορικής. Οι άγρυπνοι επιστήμονες της Silicon Valley προνοώντας το τέλμα της επεξεργαστικής ισχύος ενός παραδοσιακού κομπιούτερ, έχουν στρέψει το βλέμμα τους στους κβαντικούς υπολογιστές. Οι κβαντικοί υπολογιστές χρησιμοποιούν το qubit. 100 qubit και μόνο μπορούν να αποθηκεύσουν 1.267.650.600.288.229.401.496.703.205.375 διαφορετικούς αριθμούς, ποσότητα που αποτελεί ένα τρισεκατομμύριο φορές την αποθηκευτική ικανότητα όλων των υπολογιστών που έχουν φτιαχτεί ποτέ. [23]

Παρ' όλα αυτά, «το IoT είναι κατακερματισμένο και ακόμη στα σπάργανα», σύμφωνα με τον Luis Galvez, διευθυντή της κοινοπραξίας του Internet of Things (Internet of Things Consortium), εξηγώντας ότι υπάρχουν εταιρείες και οργανισμοί που κατασκευάζουν τις δικές τους IoT πλατφόρμες για τις δικές τους προσωπικές ανάγκες ή αυτές των πελατών τους. Ένα τρέχων παράδειγμα IoT είναι το εξής: Μια εταιρεία που ονομάζεται Rest Devices έχει δημιουργήσει ένα σετ από παιδικές πιτζάμες με ένα ειδικό μόνιτορ που σχεδιάστηκε για να ανιχνεύει το Σύνδρομο Αιφνίδιου Βρεφικού Θανάτου. Όταν ο αναπνευστικός ρυθμός του βρέφους φτάσει σε μη φυσιολογικά επίπεδα, αυτόματα στέλνεται μήνυμα στους γονείς ή γίνεται κλήση στο 911. Το σύστημα αυτό είναι αποκλειστικά ρυθμιζόμενο από τον κατασκευαστή χωρίς να μπορεί ο αισθητήρας να επικοινωνήσει για παράδειγμα με το σύστημα συναγερμού του σπιτιού ή με τα οικιακά φώτα σαν επιπρόσθετες ειδοποιήσεις. Για να γίνει αυτό, θα πρέπει η εταιρεία Rest Devices ή να κατασκευάσει τις επιπλέον αυτές συσκευές ή να συνεργαστεί με τις εταιρείες που τις κατασκευάζουν.

Για να φτάσουμε όμως να πούμε ότι το IoT έχει πραγματοποιηθεί πλήρως ή να μιλήσουμε για το πραγματικό IoT, θα πρέπει να δημιουργηθεί μια πλατφόρμα όπου όλες οι συσκευές να είναι συνδεδεμένες και να επικοινωνούν απευθείας μεταξύ τους ανεξαρτήτως κατασκευαστή ή εταιρικών συνεργασιών. Τότε ο καταναλωτής θα μπορεί να αγοράσει και αυτές τις συγκεκριμένες παιδικές πιτζάμες και το σύστημα συναγερμού και θα μπορεί να πεί «Θέλω να συνδέσω αυτά τα δύο πολύ εύκολα». Το Ίντερνετ είναι επίσης ένα πολύ καλό παράδειγμα. Ας φανταστούμε αν όλες οι συσκευές της Apple είχαν το δικό τους Ίντερνετ, συμπεριλαμβανομένων των ιστότοπων και υπηρεσιών και το ίδιο να συνέβαινε με την Samsung, την Asus και με τις υπόλοιπες εταιρείες. Τα αποτελέσματα θα απείχαν πολύ από το ισχυρό και τόσο ωφέλιμο World Wide Web που όλοι απολαμβάνουμε σήμερα. [37]

Εφαρμογές του IoT στην πραγματική ζωή

1)Το έξυπνο σπίτι (Smart Home)

Με το IoT να δημιουργεί ντόρο γύρω από το όνομά του, η φράση "Smart Home" έχει τις περισσότερες αναζητήσεις στο Google. Και ποιος δεν θα ήθελε να μπορεί να ανάψει το κλιματιστικό πριν καλά καλά φτάσει σπίτι του ή να σβήσει τα φώτα ακόμη κι αν είναι εκτός σπιτιού? Το έξυπνο σπίτι είναι μια τεχνολογική υπεροχή, της οποίας οι δυνατότητες ελέγχου, τηλε-εποπτείας και τηλεχειρισμού μιας κατοικίας είναι τεράστιες και πλήρως επεκτεινόμενες. Οι πιο σημαντικές λειτουργίες που παρέχει το «έξυπνο σπίτι», είναι η εξοικονόμηση θερμικής και ηλεκτρικής ενέργειας και η μείωση των περιβαλλοντικών ρύπων. Άλλες λειτουργίες είναι η πυρανίχνευση και η αυτόματη κατάσβεση, συστήματα ασφαλείας και πρόληψης παραβίασης, αυτόματο πότισμα, ασφαλής και εύκολος τρόπος εισόδου στο σπίτι χωρίς κλειδιά καθώς και γενικότερη διαχείριση ομάδων οικιακών συσκευών. Το παρακάτω βίντεο παρουσιάζει το πόσο απλούστερη θα είναι η ζωή σε ένα έξυπνο σπίτι. [38],[39]

2)Η τεχνολογία που φοριέται (Wearables)

Οι fans των ταινιών του James Bond ονειρεύονταν χρόνια τη στιγμή που θα μπορούσαν να φορέσουν ένα πραγματικό ρολόι με δυνατότητες επικοινωνίας, ένα δαχτυλίδι με ενσωματωμένη κάμερα ή γυαλιά που θα τους επέτρεπαν να δουν μέσα από φιμέ τζάμια. Τα wearable gadgets δεν έκαναν την εμφάνιση τους μόνο στις ταινίες, αλλά και στην πραγματική ζωή. Ο όρος wearable χρησιμοποιείται για να περιγράψει οποιοδήποτε προϊόν της τεχνολογίας έχει κατασκευαστεί για να φοριέται από καταναλωτές. Τα Wearables, διαχωρίζονται σε δύο κατηγορίες, τα Smart watches και τα Fitness Trackers. Υποστηρίζουν τις καθημερινές ανθρώπινες δραστηριότητες, όπως η επικοινωνία (διαχείριση κλήσεων, emails, SMS), αλλά και την άθληση και τη διατροφή (τρέξιμο, μέτρηση παλμών, βημάτων, υπολογισμός θερμίδων, κ.α.) Παράλληλα, τα Wearables καταγράφουν, όσα στοιχεία προεπιλέξεις και σου παρέχουν σημαντικές πληροφορίες για τις συνήθειες και τις δραστηριότητές σου, όπως για παράδειγμα την ποιότητα του ύπνου σου με στόχο της βελτίωση της καθημερινότητάς σου. Το παρακάτω βίντεο παρουσιάζει τα κορυφαία Wearables μαζί με τις δυνατότητες που προσφέρουν. [38],[40]

3)Διασυνδεδεμένα Αυτοκίνητα (Connected Cars)

Ενώ για χρόνια η αυτοκινητιστική ψηφιακή τεχνολογία είχε επικεντρωθεί στην βελτίωση των εσωτερικών διεργασιών του αυτοκινήτου, τελευταία η προσοχή έχει στραφεί στην βελτίωση της συνολικής οδηγικής εμπειρίας. Διασυνδεδεμένο αυτοκίνητο, είναι το όχημα που είναι ικανό να βελτιστοποιεί τη λειτουργία του, τη συντήρησή του, όπως επίσης και την άνεση των επιβατών του, χρησιμοποιώντας ενσωματωμένους αισθητήρες, κάμερες, ραντάρ, και σύνδεση με το Ίντερνετ. Η πλήρως αυτόνομη οδήγηση είναι το αύριο που έρχεται. Κολοσσοί όπως η Google, η Tesla, η Apple, η BMW ανταγωνίζονται στο ποια θα φέρει αυτήν την επανάσταση στα αυτοκίνητα. Με το επόμενο βίντεο, θα πάρετε μία γεύση για το μέλλον των διασυνδεδεμένων αυτοκινήτων. [38]

4)ΙΙoT, το IoT της Βιομηχανίας (Industrial IoT)

Το ΙΙoT ενσωματώνει και αξιοποιεί τεχνολογίες που υπήρχαν στο βιομηχανικό προσκήνιο εδώ και χρόνια όπως η Μηχανική Μάθηση (Machine Learning), τα Μεγάλα Δεδομένα (Big Data), οι αισθητήρες, η Διαμηχανική Επικοινωνία (Machine-to-Machine Communication) και ο αυτοματισμός. Η κύρια φιλοσοφία του ΙΙoT είναι ότι οι έξυπνες μηχανές είναι καλύτερες από τους ανθρώπους στην ακριβή και συνεχή συλλογή και δρομολόγηση των δεδομένων. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν από εταιρείες για γρηγορότερο εντοπισμό τυχόν ανεπαρκειών των μηχανών, γλιτώνοντας έτσι χρόνο και χρήμα. Επομένως το όφελος για τη βιομηχανία είναι η ανάπτυξη της παραγωγής λόγο της ολοένα και περισσότερης ζήτησης για IoT συσκευές. Το πιο σημαντικό όφελος όμως, είναι ο έλεγχος μιας εργοστασιακής μονάδας σε όλα τα σημεία. Από την ασφάλεια έως και τη σωστή κατανάλωση ρεύματος, υπάρχει πλήρης διαχείριση μέσω IoT αυτοματισμών.

Το παρακάτω βίντεο εξηγεί την ανάδυση του IoT στη βιομηχανία. [38],[42],[43]

5)Έξυπνες Πόλεις (Smart Cities)

Η έξυπνη πόλη είναι ακόμη μια ισχυρή εφαρμογή του IoT που έχει κινήσει την περιέργεια του κόσμου. Έξυπνη παρακολούθηση, αυτοματοποιημένη μετακίνηση, εξυπνότερη διαχείριση της ενέργειας και της διανομής του νερού, αστική ασφάλεια και περιβαλλοντική εποπτεία, είναι μερικά από τα παραδείγματα της εφαρμογής του IoT στις έξυπνες πόλεις. Το IoT υπόσχεται ότι θα λύσει σημαντικά προβλήματα των κατοίκων των πόλεων όπως η ρύπανση, η κυκλοφοριακή συμφόρηση, η μείωση των αποθεμάτων ενέργειας κ.α. Ένας «έξυπνος» κάδος για παράδειγμα

ενσωματώνει μια έξυπνη συσκευή η οποία διαθέτει έναν αισθητήρα πληρότητας κι ένα σύστημα επικοινωνίας μέσω του δικτύου δεδομένων κινητής τηλεφωνίας για να ειδοποιεί τις κοινοτικές αρχές για το πότε χρειάζεται να εκκενωθεί. Η κυκλοφορία θα ρυθμίζεται με τη βοήθεια ετικετών RFID στα αυτοκίνητα οι οποίες θα αποστέλλουν τα δεδομένα γεωγραφικής θέσης σε κεντρική μονάδα παρακολούθησης κ έτσι θα προσδιορίζονται οι περιοχές με συμφόρηση. Το περιβάλλον θα είναι πιο δροσερό και πιο πράσινο με λιγότερη κατανάλωση ενέργειας. Τα προβλήματα στάθμευσης μπορούν να αντιμετωπιστούν καλύτερα. Τα αυτοκίνητα θα φέρουν αισθητήρες που θα καθοδηγούν το αυτοκίνητο στις κοντινότερες διαθέσιμες θέσεις στάθμευσης. Οι πολίτες θα γνωρίζουν πάντα μέσω των smartphones την ακριβή κατάσταση των δημόσιων συγκοινωνιών και τη διαθεσιμότητά τους. Ένα έξυπνο ενεργειακό δίκτυο μπορεί να μετρήσει την παρουσία των ανθρώπων σε μια συγκεκριμένη περιοχή και ανάλογα να προσαρμόσει τα φώτα του δρόμου. Μια ελληνική εφαρμογή, βραβευμένη σε ευρωπαϊκό επίπεδο είναι το Novoville, η οποία παρέχει τη δυνατότητα σε κάθε πολίτη, να σημειώνει τα προβλήματα του Δήμου του και να τα στέλνει με το κινητό του στη δημοτική αρχή.

Για μεγαλύτερη κατανόηση της λειτουργίας των «έξυπνων» πόλεων, παρατίθεται το παρακάτω βίντεο. [38],[44]

6)Δέσμευση Ενέργειας (Energy Engagement)

Τα δίκτυα ηλεκτρικής ενέργειας του μέλλοντος δεν θα είναι μόνο έξυπνα αλλά θα είναι και αξιόπιστα. Η έννοια του έξυπνου δικτύου ηλεκτρικής ενέργειας (smart grid) κερδίζει ταχύτατα φήμη σε όλο τον κόσμο. Η κεντρική του ιδέα είναι η συλλογή δεδομένων για εποπτεία, προστασία και βελτιστοποίηση της λειτουργίας των διασυνδεδεμένων σε αυτό στοιχείων από άκρο σε άκρο. Το έξυπνο δίκτυο θα χαρακτηρίζεται από αμφίδρομη ροή ηλεκτρικής ενέργειας και πληροφοριών για τη δημιουργία ενός αυτοματοποιημένου και ευρέως κατανεμημένου δικτύου διανομής ενέργειας. Ενσωματώνει στο δίκτυο τα πλεονεκτήματα των κατανεμημένων υπολογιστικών συστημάτων και των επικοινωνιών, για τη μεταφορά σε πραγματικό χρόνο πληροφοριών με σκοπό την εξισορρόπηση της παροχής και της ζήτησης ρεύματος. Παράλληλα επιτρέπει τη διείσδυση των ανανεώσιμων πηγών ενέργειας, μειώνει σημαντικά τις εκπομπές διοξειδίου του άνθρακα και το κόστος και διορθώνει τυχόν σφάλματα (black-outs), μετατρέποντας έτσι το δίκτυο σε ένα ενεργειακό δίκτυο. Ο Jason Handley, διευθυντής της τεχνολογίας δικτύων ηλεκτρικής ενέργειας της εταιρείας Duke Energy, μιλά για έναν κόσμο όπου όλα θα είναι συνδεδεμένα μεταξύ τους, η ενέργεια θα είναι αποδοτική και όλα θα οδηγούνται από τη γνώση που παίρνουμε με τη χρήση των Προηγμένων Αναλυτικών (Advanced Analytics). Το παρακάτω βίντεο, εξηγεί τη λειτουργία του smart grid.[38],[45]

Ο ρόλος των Αναλυτικών (Analytics) στο IoT

Η Αναλυτική των Δεδομένων (Data Analytics) ορίζεται ως μια διαδικασία που χρησιμοποιείται για να εξετάσει από μικρές μέχρι και τεράστιες ροές δεδομένων (Big Data) που ποικίλουν ιδιοτήτων και να εξάγει σημαντικά συμπεράσματα από αυτά. Αυτά τα συμπεράσματα έχουν τη μορφή των τάσεων (trends), των μοτίβων (patterns) και των στατιστικών και βοηθούν επιχειρήσεις και όχι μόνο, στη λήψη αποδοτικών και επικερδών αποφάσεων. Στην περίπτωση του IoT, η Αναλυτική των Δεδομένων διαδραματίζει σημαντικό ρόλο στην ανάπτυξη και την επιτυχία του, γι αυτό και οι τεχνολογίες Αναλυτικής είναι ζωτικής σημασίας για τη μετατροπή αυτής της «πλημμύρας» δεδομένων συνεχούς ροής (streaming data) σε κατατοπιστική και χρήσιμη γνώση. Η διαδικασία ανάλυσης των δεδομένων που ρέουν ασταμάτητα μέσα από τους

αισθητήρες και τις συσκευές διαφέρουν από άλλες κοινές μεθόδους ανάλυσης που υπάρχουν σήμερα. Στην παραδοσιακή ανάλυση, τα δεδομένα αποθηκεύονται και μετά αναλύονται. Ωστόσο, στην περίπτωση των δεδομένων συνεχούς ροής όπως αυτά του IoT, τα μοντέλα και οι αλγόριθμοι είναι αυτά που αποθηκεύονται και τα δεδομένα περνούν μέσα από αυτά για ανάλυση. Αυτό το είδος ανάλυσης καθιστά δυνατό τον εντοπισμό και την εξέταση μοτίβων καθώς τα δεδομένα δημιουργούνται σε πραγματικό χρόνο. Έτσι, πριν αποθηκευτούν τα δεδομένα στο cloud ή σε οποιοδήποτε χώρο αποθήκευσης, υπόκεινται σε επεξεργασία, έπειτα χρησιμοποιείται αναλυτική ώστε να αποκρυπτογραφηθούν τα δεδομένα ενώ όλες οι συσκευές θα συνεχίσουν να εκπέμπουν και να λαμβάνουν δεδομένα. Επιπλέον, με τεχνικές προηγμένων αναλυτικών (advanced analytics), η αναλυτική των δεδομένων συνεχούς ροής μπορεί, εκτός από παρακολούθηση των υπαρχουσών συνθηκών και αξιολόγηση των κατώτατων ορίων, να κάνει πρόβλεψη μελλοντικών σεναρίων και εξέταση πολύπλοκων ερωτημάτων.

Για να εκτιμηθεί το μέλλον με τη χρήση των δεδομένων συνεχούς ροής, θα πρέπει να υπάρχουν τεχνολογίες υψηλής απόδοσης που να μπορούν να προσδιορίζουν μοτίβα στα δεδομένα τη στιγμή ακριβώς που αυτά δημιουργούνται. Μόλις ένα μοτίβο αναγνωρίζεται, μετρήσεις ενσωματωμένες στη ροή δεδομένων, οδηγούν στην αυτόματη προσαρμογή των συνδεδεμένων συστημάτων ή δημιουργούν ειδοποιήσεις για άμεσες δράσεις και λήψη καλύτερων αποφάσεων. Ουσιαστικά, αυτό σημαίνει ότι μπορούμε να προχωρήσουμε πέρα από την απλή παρακολούθηση συνθηκών και ορίων, στην εκτίμηση πιθανών μελλοντικών γεγονότων και στον προγραμματισμό τους για αμέτρητα «Τι συμβαίνει αν» (what-if) σενάρια. [3]

1.1 Δομή Διπλωματικής Εργασίας

Με την διπλωματική μου εργασία θέλω να αναδείξω τον σημαντικό ρόλο που πρόκειται να διαδραματίσει το IoT στο συναρπαστικό άμεσο μέλλον, όπου θα μετασχηματίσει τον τρόπο που αλληλεπιδρούμε μεταξύ μας, με τις συσκευές μας και τον κόσμο. Σκοπός αυτού του εγχειρήματος είναι η μια τεχνοοικονομική μελέτη και υλοποίηση ενός δικτύου κορμού με δυνατότητα σύνδεσης ετερογενών κόμβων αισθητήρων για IoT εφαρμογές. Το δίκτυο κορμού θα σχεδιαστεί με γνώμονα την ευελιξία, την επεκτασιμότητα και τη διαρκή συνδεσιμότητα, παρέχοντας παράλληλα το απαιτούμενο QoS (Quality of Service), κάνοντας πραγματικότητα τη λεγόμενη διαλειτουργικότητα.

Πιο συγκεκριμένα, στο επόμενο κεφάλαιο, πραγματοποιείται μια ανασκόπηση των τεχνολογιών WSN και IoT, παρατίθενται τα τεχνικά χαρακτηριστικά και η αρχιτεκτονική της κάθε τεχνολογίας καθώς και των τεχνολογιών που υιοθετούν. Επιπλέον, αναλύονται τα πεδία εφαρμογών των WSN/IoT και το πώς συνδέονται με την επιχειρηματικότητα. Τέλος, συζητούνται ζητήματα και απαιτήσεις ασφάλειας και ιδιωτικότητας, το νομικό πλαίσιο που διέπει τις τεχνολογίες WSN/IoT και εκρεμμή ζητήματα προς διευθέτηση.

Στο τρίτο κεφάλαιο, παρουσιάζονται οι αλγόριθμοι δρομολόγησης καθώς και τα πρωτόκολλα των WSN/IoT σε ομάδες , ανάλογα με τη λειτουργία που αυτά επιτελούν. Επίσης, συζητείται η ενεργειακά αποδοτική και ποιοτική συλλογή δεδομένων και παρουσιάζονται τα αντίστοιχα πρωτόκολλα.

Στο τέταρτο κεφάλαιο, αναφέρονται τα επιμέρους μέρη του IoT σεναρίου που υλοποιήθηκε. Αυτά περιλαμβάνουν, τα εργαλεία σχεδιασμού, προγραμματισμού και προσομοίωσης του IoT δικτύου.

Στο πέμπτο κεφάλαιο, παρουσιάζεται η υλοποίηση του IoT σεναρίου. Αρχικά, γίνεται μια τεχνοοικονομική μελέτη του αντίστοιχου ρεαλιστικού σεναρίου, σε επίπεδο κάλυψης, χωρητικότητας, ενέργειας και απόδοσης κόστους. Ακολουθεί ο σχεδιασμός του δικτύου, η διευθυνσιοδότηση των συσκευών, η τοπολογία της αρχιτεκτονικής και η δρομολόγηση του δικτύου κορμού και της IoT επέκτασης. Τέλος, εξηγείται ο σχεδιασμός της συγκεκριμένης αρχιτεκτονικής με έμφαση στην ασφάλεια σε επίπεδο αντίληψης, μεταφοράς και εφαρμογών και γίνεται η παραμετροποίηση των «έξυπνων» συσκευών.

Στο έκτο κεφάλαιο, σημειώνονται τα συμπεράσματα που εξήχθησαν από τη διενέργεια της υλοποίησης του σεναρίου του κεφαλαίου 5 και σημειώνονται κάποιες προτάσεις για μελλοντική έρευνα στην κατεύθυνση υλοποίησης IoT δικτύων 5^{ης} γενιάς.

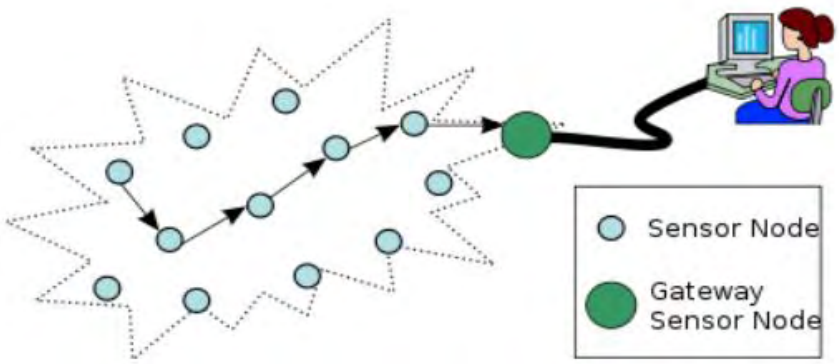
Κεφάλαιο 2: Τεχνολογίες WSN και IoT

2.1 Τεχνολογίες WSN

2.1.1 Sensors and Actuators

Τα Ασύρματα Δίκτυα Αισθητήρων (WSN-Wireless Sensor Networks) είναι ολοκληρωμένα συστήματα συλλογής, μετάδοσης και επεξεργασίας πληροφοριών. Βασικό χαρακτηριστικό τους γνώρισμα είναι ότι είναι λειτουργικά ανεξάρτητοι και ενεργειακά αυτόνομοι κόμβοι αισθητήρων, οι οποίοι τοποθετούνται (διασπείρονται) σε μια γεωγραφική περιοχή (περιορισμένης ή ευρείας έκτασης) με στόχο να μεταδώσουν πληροφορίες προς μια κεντρική μονάδα επεξεργασίας. Ο σχεδιασμός ενός WSN στηρίζεται στις δύο βασικές αρχές λειτουργίας του: τη δυνατότητα για περιοδική λήψη δεδομένων και τη δυνατότητα για εντοπισμό συμβάντων που χρίζουν άμεσης αντίδρασης/αντιμετώπισης. Η σημαντικότητα και η προτεραιοποίηση των αρχών αυτών καθορίζεται από το είδος και τις ιδιαίτερες ανάγκες της εκάστοτε εφαρμογής. [4]

Το Ασύρματο Δίκτυο Αισθητήρων είναι ο ακρογωνιαίος λίθος του IoT. Αποτελείται από πολλούς κόμβους, όπου ο καθένας από αυτούς συνδέεται σε έναν ή περισσότερους αισθητήρες οι οποίοι επικοινωνούν μεταξύ τους χρησιμοποιώντας ενσύρματα ή ασύρματα μέσα. Οι περιορισμοί σε μέγεθος και κόστος έχουν ως αποτέλεσμα αντίστοιχους περιορισμούς σε πόρους όπως ενέργεια, μνήμη, υπολογιστική ταχύτητα και στο εύρος ζώνης των επικοινωνιών. Κάθε κόμβος αισθητήρων μπορεί να διαθέτει την λειτουργία του να αισθάνεται, να επικοινωνεί και να επεξεργάζεται τα δεδομένα είτε τοπικά είτε απομακρυσμένα. Στα δίκτυα αισθητήρων, οι κόμβοι μπορούν να είναι ομογενείς ή ετερογενείς και τοποθετούνται με πυκνό τρόπο γύρω από το φαινόμενο που θέλουμε να μελετήσουμε.[4]



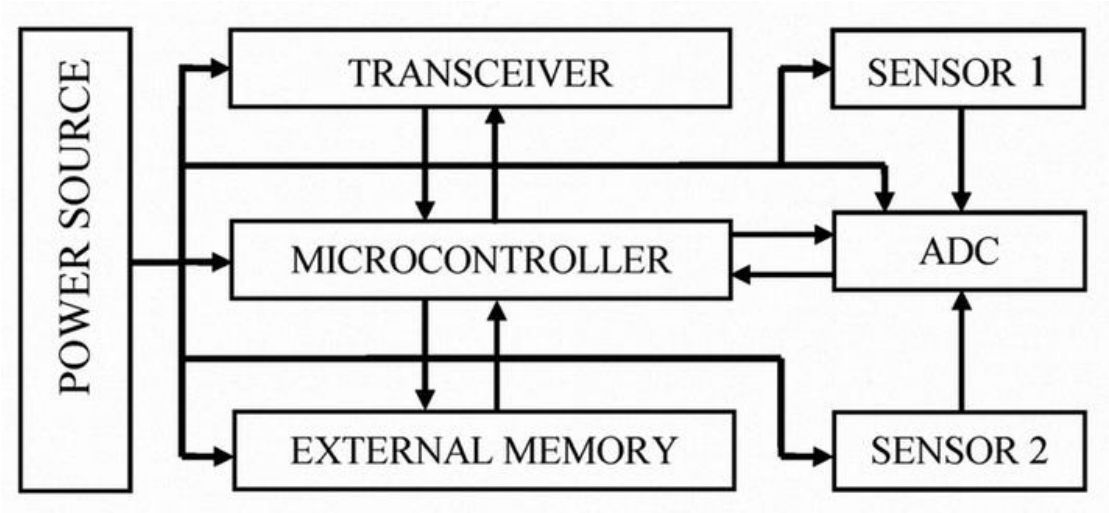
Peer to peer πολλαπλών αλμάτων (multihop) επικοινωνία ενός WSN [51]

Οι συσκευές IoT έχουν την δυνατότητα να αξιοποιούν τρισεκατομμύρια φθηνούς ασύρματους κόμβους αισθητήρων που υποστηρίζονται από το πρωτόκολλο Ίντερνετ (IP). Ο συνδυασμός οντοτήτων που αισθάνονται θα μας επιτρέψει να αλληλεπιδρούμε με το περιβάλλον γύρω μας πιο εύκολα.

Ένας αισθητήριος κόμβος μπορεί να ποικίλει σε μέγεθος από εκείνο ενός κουτιού παπουτσιών μέχρι το μέγεθος ενός κόκκου σκόνης, αν και λειτουργικοί «κόκκοι» πραγματικά

μικροσκοπικών διαστάσεων δεν έχουν ακόμα δημιουργηθεί. Το κόστος των αισθητήριων κόμβων ποικίλει, ξεκινώντας από μερικά και φτάνοντας σε εκατοντάδες δολάρια, αναλόγως την πολυπλοκότητα των μεμονωμένων αισθητήριων κόμβων. Η τοπολογία των αισθητήρων μπορεί να διαφέρει από ένα δίκτυο τοπολογίας αστέρος σε ένα αναπτυγμένο ασύρματο δίκτυο πλέγματος multi-hop. Η πολλαπλασιαστική τεχνική μεταξύ των λυκίσκων του δικτύου μπορεί να είναι η δρομολόγηση ή ο καταιγισμός διακίνησης.[51]

Ανάλογα με την εφαρμογή που καλείται να υλοποιήσει το κάθε WSN, η αρχιτεκτονική των ασύρματων κόμβων ενδέχεται να διαφέρει, αλλά τα βασικά δομικά στοιχεία του κάθε κόμβου είναι σταθερά.

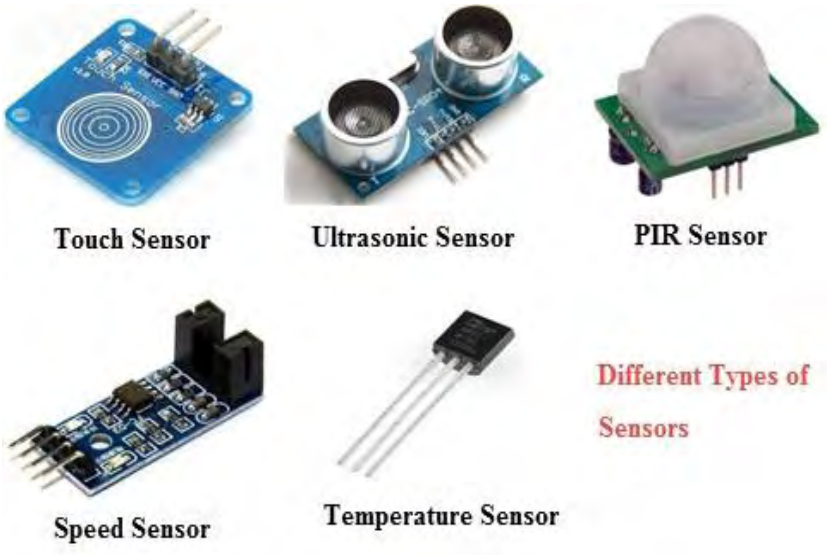


Τυπική αρχιτεκτονική ενός κόμβου αισθητήρων [53]

Έτσι, κάθε κόμβος αποτελείται από:

1. Μικροελεγκτή (Microcontroller**)**: Είναι ένα μικρό υπολογιστικό κύκλωμα, σχεδιασμένο σε ένα μόνο ολοκληρωμένο κύκλωμα υψηλής κλίμακας ολοκλήρωσης. Περιέχει κεντρική μονάδα επεξεργασίας, έναν αριθμό καταχωρητών, κυκλώματα μνήμης και κυκλώματα ελέγχου περιφερειακών συσκευών. Κάθε μικροελεγκτής είναι ικανός, να ανταλλάξει σήματα με το εξωτερικό περιβάλλον, να εκτελέσει πράξεις και να καταχωρήσει κάποιες τιμές στη μνήμη RAM που διαθέτει. [52] Ο μικροελεγκτής αποτελεί το κεντρικό δομικό στοιχείο κάθε «έξυπνης» συσκευής και είναι υπεύθυνος για το συγχρονισμό και την εκτέλεση όλων των λειτουργιών του συστήματος. Μέσω αυτού οι συσκευές επεξεργάζονται, στέλνουν ή λαμβάνουν πληροφορία. Σε κάποιες συσκευές μπορούμε να συναντήσουμε αντί για μικροελεγκτή, μικροεπεξεργαστές γενικού σκοπού όπως FPGA, DSP, ASIC αλλά συνήθως δεν αποτελούν τη βέλτιστη λύση σε θέματα κατανάλωσης ενέργειας, κόστους, ευκολίας προγραμματισμού και συνεργασίας με το υπόλοιπο σύστημα.[53]
2. Μνήμη (External Memory): Συνήθως χρησιμοποιείται η μνήμη FLASH σε συνδυασμό με τη μνήμη του chip του μικροελεγκτή λόγω χαμηλής κατανάλωσης σε σχέση με τη RAM. Σε αρκετούς κόμβους παρατηρούμε να γίνεται διαχωρισμός της μνήμης που αφορά τον προγραμματισμό του κόμβου και της περιοχής που αποθηκεύονται δεδομένα και εφαρμογές του χρήστη.[53]

3. Πηγή Ενέργειας (Power Source**):** Ένας ασύρματος κόμβος αισθητήρων βρίσκεται συχνά σε απρόσιτες περιοχές, όπου το να αλλάζεις την μπαταρία συχνά είναι πολυέξοδο και κουραστικό. Για το WSN το πιο ζωτικό κομμάτι του σχεδιασμού του είναι να υπάρχει αρκετή ενέργεια που θα τροφοδοτεί το σύστημα. Ο κόμβος καταναλώνει ενέργεια για την «αίσθηση», την επικοινωνία και την επεξεργασία των δεδομένων. Η περισσότερη ενέργεια που καταναλώνει είναι κατά την επικοινωνία των δεδομένων (data communication). Η ενέργεια αυτή παρέχεται από μπαταρίες και πυκνωτές. Σύγχρονοι κόμβοι αισθητήρων χρησιμοποιούν ανανεώσιμες πηγές ενέργειας όπως η ηλιακή ενέργεια, η διαφορές της θερμοκρασίας και οι δονήσεις της συσκευής. [53]
4. Κεραία ή πομποδέκτης (Transceiver): Η κεραία δίνει τη δυνατότητα στους κόμβους να επικοινωνούν μεταξύ τους ή με άλλες συσκευές ασύρματα. Οι κόμβοι αισθητήρων κάνουν συνήθως χρήση της μπάντα συχνοτήτων ISM (Industrial, Scientific and Medical radio bands), η οποία προσφέρει ελεύθερη (χωρίς αδειοδότηση) ραδιοεπικοινωνία, κατανομή φάσματος και παγκόσμια διαθεσιμότητα. Η επικοινωνία μπορεί να επιτευχθεί με Ραδιοσυχνότητες (RF), με Οπτική Επικοινωνία (Laser) και με Υπέρυθρη Ακτινοβολία (IR). Η επικοινωνία μέσω Laser απαιτεί λιγότερη ενέργεια αλλά απαιτεί οπτική επαφή που δεν είναι πάντα εφικτό και είναι ευαίσθητη σε περιβαλλοντικές συνθήκες. Η επικοινωνία μέσω IR όπως και με Laser δεν απαιτεί antenna αλλά έχει περιορισμένη ικανότητα μετάδοσης. Γι αυτούς τους λόγους η καταλληλότερη επικοινωνία για WSN γίνεται με Ραδιοσυχνότητες. Τα WSN κάνουν χρήση «ελεύθερων» συχνοτήτων όπως: 173, 433, 868, 915 MHz και 2,4 GHz. Τα στάδια λειτουργίας του πομποδέκτη είναι μετάδοση, λήψη, αδράνεια, «ύπνος» και καταναλώνει μεγάλο ποσό ενέργειας κατά τη διάρκεια μετάβασης από τον ύπνο στην μετάδοση όταν χρειάζεται να μεταδώσει ένα πακέτο. [53]
5. Αισθητήρες (Sensors): Οι Αισθητήρες χρησιμοποιούνται από τους ασύρματους κόμβους αισθητήρων για να συλλέξουν πληροφορίες από το περιβάλλον. Αποτελούν συσκευές που ανιχνεύουν ένα φυσικό μέγεθος και παράγουν από αυτό μια μετρήσιμη έξοδο ως απάντηση στην μεταβολή μιας φυσικής κατάστασης για παράδειγμα θερμοκρασίας ή πίεσης. Το συνεχές αναλογικό σήμα που παράγεται από τους αισθητήρες μετατρέπεται σε ψηφιακό από έναν ανάλογο μετατροπέα και στέλνεται στους μικροελεγκτές για περαιτέρω επεξεργασία. Κάποιοι αισθητήρες είναι κατασκευασμένοι με τα απαραίτητα ηλεκτρονικά συστήματα για να μετατρέπουν τα ακατέργαστα (raw) σήματα σε readings και αρκετοί μετατρέπουν τα σήματα σε μονάδες όπως οι βαθμοί Κελσίου (°C). Οι περισσότεροι αισθητήρες είναι μικροί σε μέγεθος, καταναλώνουν λίγη ενέργεια, λειτουργούν σε υψηλές ογκομετρικές πυκνότητες, είναι αυτόνομοι και λειτουργούν χωρίς επιτήρηση, καθώς και προσαρμόζονται στο περιβάλλον.

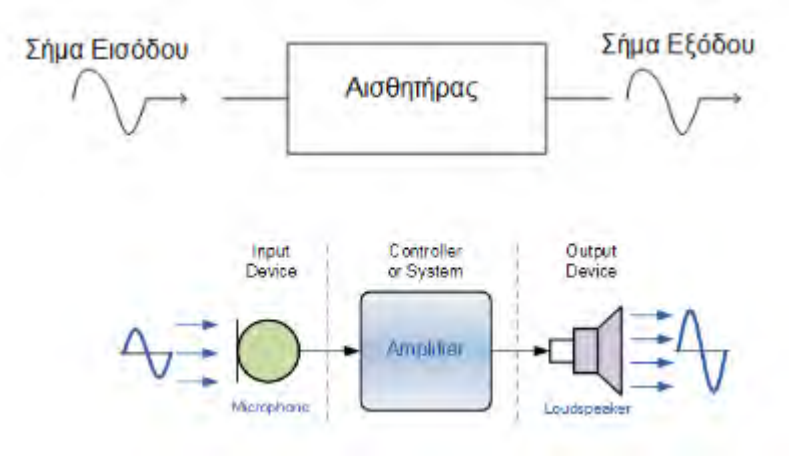


Τύποι αισθητήρων[54]

Ανάλογα με την επιρροή των αισθητήρων στο περιβάλλον τους, οι αισθητήρες κατηγοριοποιούνται ως εξής:

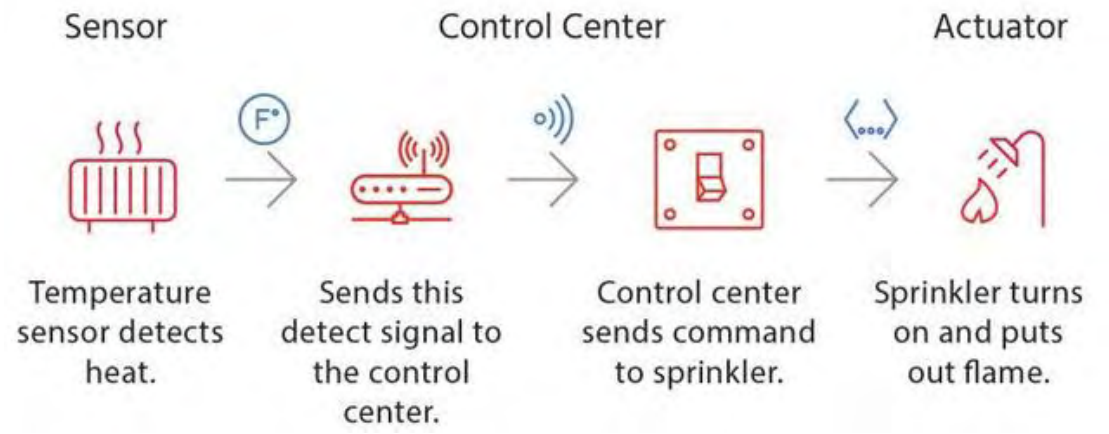
1. Παθητικοί: Δεν επεμβαίνουν στο περιβάλλον, δηλαδή δεν εκπέμπουν κάποια μορφή ενέργειας αλλά μετρούν την ενέργεια που προέρχεται από κάποια φυσική πηγή. Συνήθως για να πετύχουμε αυτή την ιδιότητα, σχεδιάζουμε τους αισθητήρες πολύ μικρούς με τη χρήση της τεχνολογίας MEMS. Οι παθητικοί αισθητήρες χωρίζονται επίσης σε δύο κατηγορίες:
   - Γενικής κατεύθυνσης: Οι αισθητήρες αυτοί συλλέγουν συγκεκριμένες πληροφορίες για το περιβάλλον γύρω τους από όλες τις κατευθύνσεις όπως για παράδειγμα ένας αισθητήρας θερμοκρασίας.
   - Συγκεκριμένης κατεύθυνσης: Οι αισθητήρες αυτοί συλλέγουν πληροφορίες από μια συγκεκριμένη κατεύθυνση, όπως για παράδειγμα μια κάμερα.
2. Ενεργητικοί: Επεμβαίνουν στο περιβάλλον για να μετρήσουν κάποιο φυσικό μέγεθος, δηλαδή εκπέμπουν κάποια μορφή ενέργειας (κύματα ήχου, φωτός κ.α) στο περιβάλλον , με σκοπό να μετρήσουν τις αλλαγές που προκύπτουν στην εκπεμπόμενη ενέργεια. Εκπέμπουν και μετρούν ταυτόχρονα. Χαρακτηριστικό παράδειγμα ενεργητικού αισθητήρα είναι το SONAR, οι ενεργητικοί υπέρυθροι αισθητήρες (InfraRed) κ.α.

Σε ένα τυπικό IoT δίκτυο, ένας αισθητήρας μπορεί να συλλέγει πληροφορίες και να τις δρομολογεί σε ένα κέντρο ελέγχου προκειμένου να παρθεί μια απόφαση. Τότε μια αντίστοιχη εντολή θα δοθεί από το κέντρο ελέγχου προς έναν ενεργοποιητή (actuator) ως απάντηση του εισερχόμενου ερεθίσματος που έλαβε ο αισθητήρας.



Αισθητήρας [58]

Ο **ενεργοποιητής** (actuator) είναι μία συσκευή η οποία ενεργοποιεί ή κινεί κάτι. Συνεπώς ο ρόλος του είναι να μετατρέπει την ενέργεια σε κίνηση (μετατόπιση) ή σε μηχανική ενέργεια (τάση). Οι ενεργοποιητές για τη σωστή τους λειτουργία, θα πρέπει να είναι διανεμημένοι σε όλο το εύρος της δομής. Οι ενεργοποιητές μπορούν να δημιουργήσουν γραμμική, ταλαντευόμενη ή περιστροφική κίνηση, ανάλογα με το σχεδιασμό τους.



Η διαδρομή από τον αισθητήρα στον ενεργοποιητή [55]

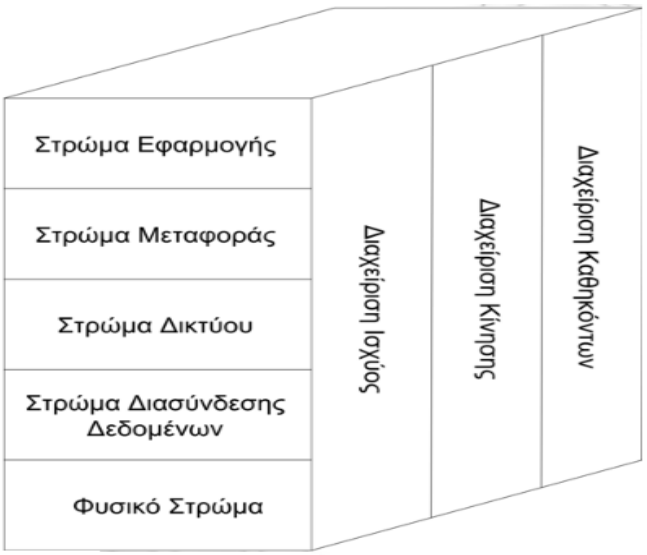
Η τάση που προκαλείται από έναν ενεργοποιητή καλείται τάση ενεργοποίησης. Υπάρχουν πολλοί τρόποι με τους οποίους μπορούν να εφαρμοστούν οι τάσεις ενεργοποίησης, όπως οι αλλαγή της θερμοκρασίας, η έκθεση σε υγρασία, αλλά μόνο μερικοί από αυτούς είναι χρήσιμοι και δυνατό να ελεγχθούν. Συνηθέστεροι τρόποι εφαρμογής μιας τάσης σε μια δομή μέσω ενός ενεργοποιητή είναι ο πιεζοηλεκτρισμός, η ηλεκτροσυστολή, η μαγνητοσυστολή, και η επίδραση μνήμης μορφής. Στο IoT, οι ενεργοποιητές χρησιμοποιούνται κάθε φορά που χρειάζεται να ανοίξουμε/κλείσουμε μια άλλη συσκευή ή εξοπλισμό χρησιμοποιώντας δύναμη. [57]

Ας σκεφτούμε μια υποθετική περίπτωση όπου θα θέλαμε η αντλία νερού μας να ανοίξει όταν το επίπεδο νερού της δεξαμενής πέσει κάτω από ένα επίπεδο. Πώς θα σχεδιάζαμε αυτό το σύστημα? Θα είχαμε έναν αισθητήρα να παρατηρεί το επίπεδο του νερού και όταν η στάθμη έπεφτε κάτω από ένα όριο, τότε ο αισθητήρας θα έστελνε μια ειδοποίηση στον ελεγκτή. Ο

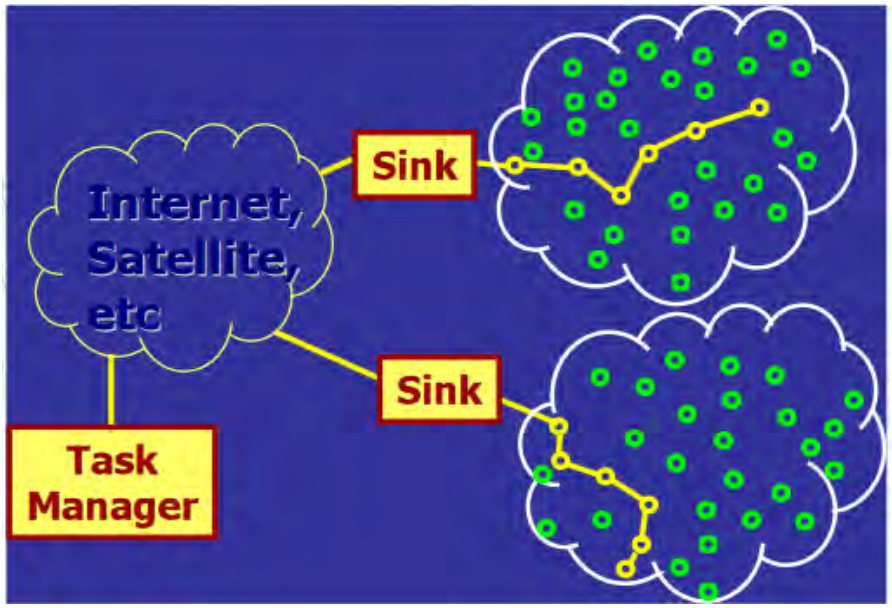
ελεγκτής με τη σειρά του θα έθετε σε ενέργεια τον ενεργοποιητή ώστε να ανοίξει την αντλία νερού. [58]

2.1.2 Τεχνολογίες και πρωτόκολλα πρόσβασης

Η λειτουργία των WSNs, όπως και όλων των ασύρματων δικτύων, βασίζεται στον καταμερισμό των εργασιών σε διαφορετικά στρώματα ή επίπεδα (layers). Η διαδικασία αυτή καλείται διαστρωμάτωση, και μια αναλυτική παρουσίαση των εργασιών που αναλαμβάνει κάθε στρώμα μπορεί να βρεθεί στο [1]. Συνοπτικά, τα στρώματα που συμμετέχουν στην μετάδοση ενός πακέτου πληροφορίας είναι το φυσικό στρώμα, το στρώμα διασύνδεσης δεδομένων, το στρώμα δικτύου, το στρώμα μεταφοράς και το στρώμα εφαρμογής. Η δομή ενός WSN και η διασύνδεσή του με άλλα υπάρχοντα δίκτυα περιγράφεται συνοπτικά από την εικόνα τάδε. Κατά κανόνα, όταν ένας αισθητήρας λαμβάνει κάποια πληροφορία από το περιβάλλον, στη συνέχεια την μεταδίδει στο δίκτυο μέσω πολλαπλών βημάτων (hops). Η πληροφορία τελικά καταλήγει σε έναν μεγαλύτερης πολυπλοκότητας κόμβο– μεσολαβητή (SINK) ο οποίος στη συνέχεια την προωθεί σε άλλο δίκτυο, μέχρι τελικά να φτάσει στον τελικό χρήστη.



Διαστρωμάτωση WSN [2]



Δομή του WSN και σύνδεση του με άλλα δίκτυα [2]

Οι ασύρματες τεχνολογίες μπορούν να χωριστούν σε διάφορες κατηγορίες, σύμφωνα με κριτήρια όπως:

- Το πρωτόκολλο που χρησιμοποιούν
- Το είδος σύνδεσης
- Το φάσμα συχνοτήτων στο οποίο λειτουργούν.

Το κύριο χαρακτηριστικό είναι η δυνατότητα ασύρματης δικτύωσης με χαμηλή κατανάλωση ενέργειας, ώστε να είναι εφικτή η υλοποίηση εφαρμογών, σε περιοχές όπου η πρόσβαση στον αισθητήριο κόμβο είναι δύσκολη. Φυσικά υπάρχουν εφαρμογές οι οποίες έχουν υλοποιηθεί με πρότυπα τα όποια δεν προσφέρουν εξοικονόμηση ενέργειας. Το γεγονός αυτό δεν καθιστά μη αποτελεσματικές αυτές τις εφαρμογές. Για την υλοποίηση ενός WSN, ο σχεδιαστής της εφαρμογής επιλέγει ένα από τα πολλά πρότυπα που έχουν δημιουργήσει διάφοροι οργανισμοί και εταιρείες τα τελευταία χρόνια. Στη συνέχεια αναφέρονται τα κυριότερα:

Το πρότυπο IEEE 802.15.4

Το IEEE 802.15.4 αποτελεί το περισσότερο ευρέως εν χρήσει πρότυπο για τα WSN δίκτυα και κατ'επέκταση για το IoT στο επίπεδο MAC. Ορίζει τη δομή του πλαισίου (frame), τις επικεφαλίδες συμπεριλαμβανομένων των διευθύνσεων πηγής και προορισμού και επίσης το πώς οι κόμβοι μπορούν να επικοινωνούν ο ένας με τον άλλον. [138]

Το IEEE 802.15.4 εξυπηρετεί ένα σύνολο βιομηχανικών, οικιακών και ιατρικών εφαρμογών με πολύ χαμηλή κατανάλωση ενέργειας λόγω του χαμηλού ρυθμού μετάδοσης δεδομένων και πάνω του στηρίζονται το ZigBee, το WirelessHART και το ISA100.11a [80].

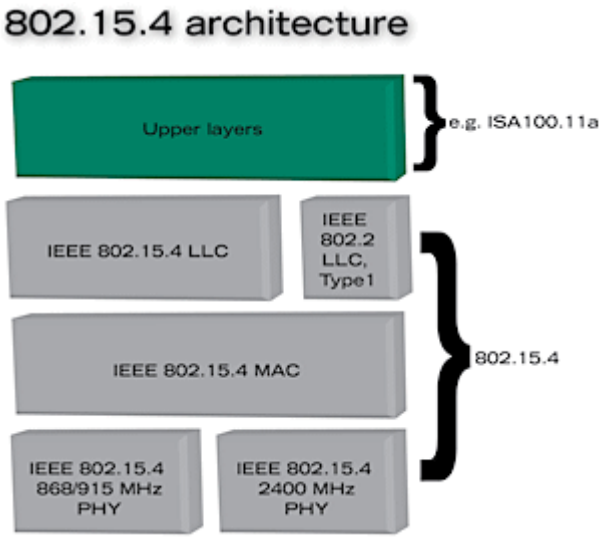
Το IEEE 802.15.4 ολοκληρώθηκε στις αρχές του 2003 και είναι ένα πρότυπο που ορίζει το φυσικό στρώμα (PHY Layer) και τον έλεγχο πρόσβασης μέσου (MAC) για ασύρματα προσωπικά δίκτυα μικρής εμβέλειας και χαμηλής ταχύτητας (LR WPANs- Low Rate Wireless Personal Area Networks) που σχηματίζονται από σταθερές ή κινούμενες συσκευές, τροφοδοτούμενες από μπαταρίες ή κάποια άλλη πηγή περιορισμένης ενέργειας χωρίς όμως να

υποστηρίζει ανώτερα στρώματα ή μεθόδους δικτύωσης. Το βασικότερο συστατικό των δικτύων που χρησιμοποιούν το πρότυπο 802.15.4 είναι η συσκευή ή κόμβος. Υπάρχουν δύο είδη κόμβων:

- Συσκευή πλήρους λειτουργίας (Full Function Device– FFD) και
- Συσκευή μειωμένης λειτουργίας (Reduced Function Device– RFD)

[80]

Η αρχιτεκτονική κάθε LR-WPAN στην κατηγορία των οποίων ανήκουν και τα WSNs (Wireless Sensor Networks), κατηγοριοποιείται σε μια σειρά από επίπεδα, τα οποία διευκολύνουν τη μελέτη και το σχεδιασμό του δικτύου. Αποτελείται από το φυσικό επίπεδο, το οποίο περιλαμβάνει έναν πομποδέκτη για τις ράδιο-συχνότητες μαζί με κάποιους μηχανισμούς ελέγχου χαμηλού επιπέδου, και το επίπεδο MAC, το οποίο παρέχει μηχανισμούς πρόσβασης στο φυσικό κανάλι, όπως το CSMA/CA (Carrie Sense Multiple Access/ Collision Avoidance). Η πρόσβαση στο υπό-επίπεδο MAC γίνεται μέσω του Logical Link Control (LLC) και της ειδικής υπηρεσίας σύγκλισης του υπό επιπέδου (Service Specific Convergence Sublayer- SSCS).[80]



Η αρχιτεκτονική του προτύπου IEEE 802.15.4 [80]

Το φυσικό επίπεδο παρέχει δύο υπηρεσίες, την υπηρεσία δεδομένων (PHY data service) και την υπηρεσία διαχείρισης (PHY management service), που αλληλοεπιδρά με την οντότητα διαχείρισης του φυσικού επιπέδου (Physical Layer Management Entity– PLME).
Τα χαρακτηριστικά του PHY επιπέδου του 802.15.4 είναι [80]:

- Ενεργοποίηση και Απενεργοποίηση του Πομποδέκτη, όπου αυτός τίθεται σε μια από τις τρεις καταστάσεις: εκπομπή, λήψη και sleep
- Ανίχνευση Ενέργειας (Energy Detection– ED) , όπου πρόκειται για μια εκτίμηση της ισχύος του λαμβανόμενου σήματος εντός του εύρους ζώνης του πρωτοκόλλου IEEE 802.15.4
- Ένδειξη Ποιότητας Ζεύξης (Link Quality Indication – LQI)
- Επιλογή συχνότητας καναλιού, αφού οι ασύρματες ζεύξεις μπορούν να λειτουργήσουν σε 27 διαφορετικά κανάλια υπό το πρότυπο 802.15.4 και έτσι το φυσικό επίπεδο είναι υπεύθυνο για τη μετάθεση του πομποδέκτη σε ένα συγκεκριμένο κανάλι
- Έλεγχος Αδράνειας Καναλιού (Clear Channel Assessment - CCA)

- Αποστολή και λήψη δεδομένων.

Το επίπεδο έλεγχου πρόσβασης μέσου-MAC εξασφαλίζει την διασύνδεση των ανώτερων επιπέδων με το φυσικό. Είναι το επίπεδο που ελέγχει άμεσα το PHY. Οι αρμοδιότητές του είναι:

- Η παραγωγή των beacons
- Ο συγχρονισμός των συσκευών στο εισερχόμενο beacon
- Να επιτρέπει την σύνδεση και την αποσύνδεση μεταξύ των συσκευών στα ZigBee δίκτυα
- Να υποστηρίζει τις παραμέτρους ασφαλείας του πρωτοκόλλου
- Να χρησιμοποιεί CSMA-CA για να επιτρέψει την πρόσβαση στο κανάλι
- Η παραχώρηση των GTS (Guaranteed Time Slots) [81],[82]

Στον παρακάτω πίνακα παρουσιάζονται συνοπτικά οι διαφορετικές ζώνες συχνοτήτων, οι αριθμοί καναλιών , οι διαμορφώσεις και οι ρυθμοί δεδομένων που υποστηρίζουν.

PHY (MHz)	Ζώνη Συχνοτήτων (MHz)	Παράμετροι Διάδοσης		Παράμετροι Δεδομένων			Κανάλια
		Ρυθμός Chip (kchip/s)	Διαμόρφωση	Ρυθμός Bit (kb/s)	Ρυθμός Συμβόλων (ksymbols/s)	Σύμβολα	
868/915	868-868,6	300	BPSK	20	20	Binary	1
	902-928	600	BPSK	40	40	Binary	10
2450	2400-2483,5	2000	O-QPSK	250	62,5	16-ary Orthogonal	16

Ergen S.C., (2004), ZigBee/IEEE 802.15.4 Summary [80]

Στο πρωτόκολλο 802.15.4 εκχωρούνται συνολικά 27 κανάλια εκ των οποίων 16 κανάλια ανήκουν στη ζώνη των 2.4GHz σε παγκόσμιο επίπεδο, 10 στη ζώνη μεταξύ 902 και 928MHz για την Αμερική και 1 κανάλι στη ζώνη μεταξύ 868 και 868.8 MHz για την Ευρώπη. Η ζώνη των 2.4GHz αποτελεί την πιο διαδεδομένη ζώνη συχνοτήτων, που είναι και η κοινή ζώνη συχνοτήτων λειτουργίας με τα υπόλοιπα ασύρματα δίκτυα και στις τρεις ζώνες. [80]

EnOcean

Το EnOcean είναι μια ασύρματη τεχνολογία χαμηλής κατανάλωσης ενέργειας η οποία βρίσκει εφαρμογή κυρίως σε συστήματα αυτοματισμού κτιρίων. Το πρότυπο είναι ιδιωτικό, ωστόσο η EnOcean GmbH προσφέρει την τεχνολογία της και την άδεια για τα κατοχυρωμένα χαρακτηριστικά του προϊόντος της. Το πρότυπο αναπτύχθηκε για την δημιουργία αισθητήρων και διακοπτών για κτιριακούς αυτοματισμούς οι οποίοι θα λαμβάνουν ενέργεια από μετατροπή φυσικών φαινομένων.

Τα προϊόντα που συμμορφώνονται με το πρότυπο EnOcean δεν χρειάζονται συσσωρευτές και κατασκευάζονται για να λειτουργήσουν χωρίς την ανάγκη συντήρησης. Η παροχή ενέργειας επιτυγχάνεται με μετατροπή ηλιακής, αιολικής, ηλεκτρομαγνητική, πιεζοηλεκτρική ενεργείας κ.α. Τα σήματα από αυτούς τους αισθητήρες και διακόπτες μπορούν να διαβιβαστούν ασύρματα

σε εμβέλεια μέχρι 300 μέτρα. Η διαβίβαση των μηνυμάτων γίνεται με εκπομπή ραδιοκυμάτων σε χρονικό διάστημα ενός δευτερόλεπτου, ώστε να εξοικονομείται ενέργεια. Κατά την εκπομπή, για την αποφυγή πιθανών συγκρούσεων ακολουθείται η τακτική να στέλνονται τρία πακέτα σε ψευδοτυχαία διαστήματα. Η μετάδοσης των δεδομένων γίνεται στις ζώνες των 868.3 MHz και 315 MHz. Η EnOcean GmbH είναι προμηθευτής τεχνολογίας αυτοτροφοδοτούμενων συσκευών σε εταιρίες, οι οποίες αναπτύσσουν και κατασκευάζουν προϊόντα τα οποία χρησιμοποιούνται στην αυτοματοποίηση κτιρίων (HVAC), σε βιομηχανίες αυτοματοποίησης και σε αυτοκινητοβιομηχανίες. [63],[64],[65]

DASH7

Το DASH7 είναι ένα ανοικτό πρότυπο δικτύωσης αισθητήρων από την μη κερδοσκοπική κοινοπραξία που ονομάζεται DASH7 Alliance. Ακολουθεί το ανοικτό πρότυπο ISO/IEC 18000-7 για την παγκοσμίως ελεύθερη ζώνη συχνοτήτων 433 MHz στις ασύρματες επικοινωνίες. Η τεχνολογία DASH7 δημιουργήθηκε αρχικά για στρατιωτική χρήση στην πορεία όμως έχει χρησιμοποιηθεί και για άλλες εμπορικές εφαρμογές. Τα χαρακτηριστικά που διακρίνουν το DASH7 είναι η πολυετή διάρκεια ζωής της μπαταρίας (έως 10 χρόνια), η εμβέλεια μέχρι 2 Km, ο μικρός χρόνος αναμονής κατά τη σύνδεση, η υποστήριξη για κλειδί κρυπτογράφησης AES 128-bit και η μεταφορά δεδομένων με ρυθμό μέχρι 200 Kbps. Σοβαρό πλεονέκτημα της τεχνολογίας DASH7 είναι ότι τα σήματα μπορούν να διαπεράσουν το σκυρόδεμα και το νερό και να ταξιδέψουν σε πολύ μεγάλες αποστάσεις χωρίς να απαιτείται μεγάλη κατανάλωση ενέργειας. [66],[67]

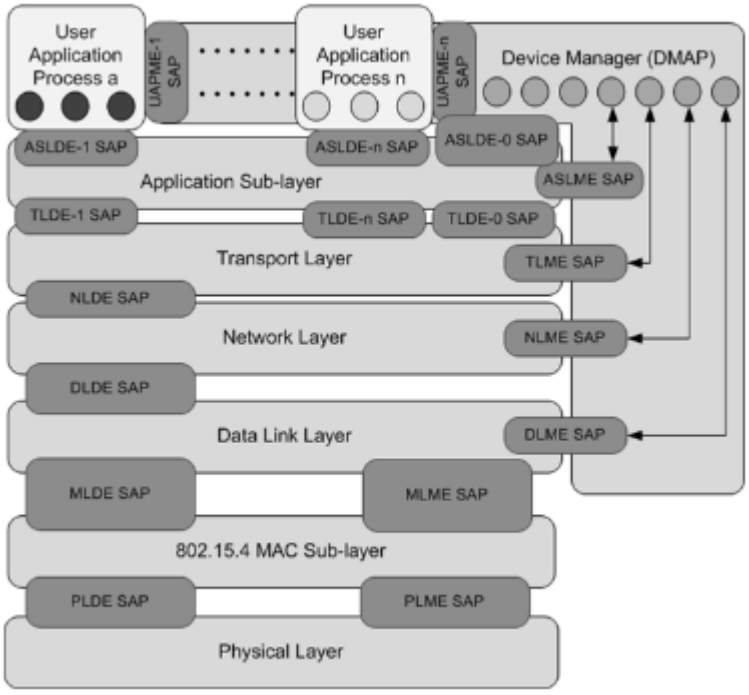
RuBee

Το RuBee είναι ένα πρότυπο ασύρματης επικοινωνίας το οποίο χρησιμοποιεί μαγνητικά σήματα μακρών κυμάτων για την αποστολή και λήψη των πακέτων δεδομένων. Έχει σχεδιαστεί για να χρησιμοποιηθεί σε περιβάλλοντα με θορύβους σε εφαρμογές υψηλής ασφάλειας, ενώ είναι η μοναδική ασύρματη τεχνολογία η οποία έχει πάρει έγκριση από το Υπουργείο Ενέργειας των ΗΠΑ για χρήση σε ασφαλείς εγκαταστάσεις και σε περιοχές εκρήξεων. Χρησιμοποιεί μικρό μέγεθος πακέτων δεδομένων, 128 byte, στη ζώνη συχνοτήτων των 131 KHz. Το πρότυπο έχει ομοιότητες με τα πρωτόκολλα IEEE 802 (όπως WiFi - IEEE 802.11, WPAN -IEEE 802.15.4 και Bluetooth- IEEE 802.15.1). Βέβαια, η διαφορά είναι ότι χρησιμοποιεί μαγνητικά σήματα ενώ τα περισσότερα πρότυπα ασύρματης δικτύωσης χρησιμοποιούν ηλεκτρικά σήματα. Συνέπεια αυτού είναι το RuBee να έχει χαμηλό ρυθμό μεταφοράς δεδομένων, 1.200 bps. Η χαμηλή συχνότητα λειτουργίας παρέχει βέβαια στο RuBee το πλεονέκτημα της εξαιρετικά χαμηλής κατανάλωσης ενέργειας, συνεπώς η διάρκεια ζωής της μπαταρίας των συσκευών ανέρχεται σε πολλά χρόνια. Επιπλέον η λειτουργία του σ’ αυτή τη ζώνη συχνοτήτων έχει αποτέλεσμα το RuBee να μην έχει αντανακλάσεις και να μην εμποδίζεται από χάλυβα ή υγρά, γεγονός που το καθιστά αποτελεσματικότερο σε αντίξοες συνθήκες περιβάλλοντος και σε εφαρμογές ασφαλείας. Ένα πλεονέκτημα ακόμα είναι η λειτουργία του χωρίς προβλήματα κάτω από οποιεσδήποτε καιρικές συνθήκες και ο μικρός κίνδυνος υποκλοπών. [68],[69]

Isa100.11a

Το ISA100.11a είναι ένα πρότυπο ανοιχτού κώδικα για ασύρματα δίκτυα αισθητήρων από την διεθνή κοινότητα αυτοματισμού (International Society of Automation– ISA). Το ISA100.11a έχει δημιουργηθεί για χρήση σε βιομηχανικά δίκτυα ασύρματων αισθητήρων, ενώ επιτρέπει την επικοινωνία με άλλα ήδη υπάρχοντα ασύρματα και ενσύρματα δίκτυα. Χρησιμοποιεί την ελεύθερη ζώνη συχνοτήτων 2,4 GHz για την αποστολή μηνυμάτων, με ρυθμό μεταφοράς δεδομένων 250 kbps, σε τοπολογίες πλέγματος και δέντρου. Είναι ανθεκτικό στον θόρυβο που υπάρχει στα βιομηχανικά περιβάλλοντα και υποστηρίζει κρυπτογράφησης AES 128-bit.

Αποτελείται από τα επίπεδα εφαρμογής, μεταφοράς, δικτύου, σύνδεσης δεδομένων, ενώ τα επίπεδα έλεγχου πρόσβασης μέσου (MAC) και το φυσικό (PHY) ορίζονται από το πρότυπο 802.15.4. Εικόνα τάδε. Το επίπεδο δικτύου χρησιμοποιεί επικεφαλίδες οι οποίες είναι συμβατές με το πρότυπο 6LoWPAN ενώ το επίπεδο μεταφοράς υποστηρίζει τις υπηρεσίες ασφάλειας, αυθεντικοποίησης, και κρυπτογράφησης του πρωτοκόλλου IPv6. Στο επίπεδο εφαρμογής καθορίζονται τα αντικείμενα και ορίζονται οι υπηρεσίες επικοινωνιών, που είναι αναγκαίες, ώστε να επικοινωνούν τα αντικείμενα μεταξύ τους, σε κατανεμημένες εφαρμογές.



Αρχιτεκτονική επιπέδων του ISA100.11a [71]

Ένα τυπικό δίκτυο ISA 100.11a μπορεί να αποτελείται από επτά τύπους συσκευών: την πύλη (gateway), τον διαχειριστή του συστήματος (system manager), τον διαχειριστή ασφάλειας (security manager), τον δρομολογητή (router), τον δρομολογητή κορμού (Backbone router), τις συσκευές εισόδου/εξόδου (input/output IO devices) και τις φορητές συσκευές (portable devices). Κάθε συσκευή εκτελεί ένα συγκεκριμένο ρόλο στην λειτουργία του δικτύου. Ανάλογα με την ρύθμιση που έχει επιλεγεί, επηρεάζεται και η κατανάλωση ενέργειας. Το ISA 100.11a υποστηρίζει μεταφορά δεδομένων με διαίρεση χρόνου (TDMA), με πολλαπλή πρόσβαση με ανίχνευση φέροντος (CSMA) και με ένα υβριδικό συνδυασμό των δυο. [70-74]

6LoWPAN

Το 6LoWPAN είναι ένα ανοιχτό πρότυπο από την ομάδα εργασίας IETF. Το όνομα του προέρχεται από τα αρχικά των λέξεων IPv6 over Low power Wireless Personal Area Networks. Σκοπός του 6LoWPAN είναι ο καθορισμός των κριτηρίων για την εδραίωση επικοινωνιών IP πάνω σε συνδέσεις IEEE 802.15.4 με τρόπο που να συμμορφώνεται στα ανοικτά πρότυπα και να παρέχει διαλειτουργικότητα σε άλλες IP συνδέσεις και συσκευές καθώς και σε συσκευές IEEE 802.15.4 Το 6LoWPAN υλοποιεί την σκέψη ότι το πρωτόκολλο του διαδικτύου θα πρέπει να είναι εφαρμόσιμο και να συνδέει διαδικτυακά ακόμη και τις μικρότερες συσκευές χαμηλής ισχύος και επεξεργαστικής δυνατότητας. Στο 6LoWPAN καθορίζεται η δομή και οι μηχανισμοί ενθυλάκωσης και συμπίεσης των επικεφαλίδων ώστε να επιτρέπεται σε πακέτα IPv6 να κυκλοφορούν σε δίκτυα βασισμένα στο πρωτόκολλο IEEE 802.15.4. Το 6LoWPAN ορίζει τα ανώτερα επίπεδα του δικτύου ενώ τα κατώτερα, PHY και MAC, ορίζονται από το πρότυπο IEEE 802.15.4. Υποστηρίζει τοπολογία αστέρα, πλέγματος και συνδυασμούς των δυο. Η αποστολή δεδομένων γίνεται με μικρά πακέτα των 128 byte, με ρυθμό μεταφοράς δεδομένων από 20 kbps έως 250 kbps σε απόσταση 10 έως 30 μέτρων, εξαρτώμενα από την επιλεγμένη συχνότητα λειτουργίας και διαμόρφωση του πρότυπου IEEE 802.15.4. Επίσης υποστηρίζονται διάφορες μέθοδοι κρυπτογράφησης AES με υποχρεωτική την AES-CCM-64. [75],[76]

WirelessHART

Το WirelessHART είναι το πρώτο ανοιχτό πρότυπο βιομηχανικής ασύρματης επικοινωνίας, που σχεδιάστηκε ως ασύρματη επέκταση του πρωτοκόλλου HART (Highway Addressable Remote Transducer) το Σεπτέμβριο του 2007 από την HART Communication Foundation (HCF) [99]. Το WirelessHART προσφέρει απλότητα, ευρωστία, χαμηλότερο κόστος εγκατάστασης και συντήρησης και περισσότερη ευελιξία στην διαμόρφωση στις βιομηχανικές εφαρμογές αυτοματισμού και ελέγχου από το HART [101]. Το WirelessHART είναι μια ασύρματη τεχνολογία δικτύωσης η οποία λειτουργεί στη μη αδειοδοτημένη ζώνη συχνοτήτων 2.4 GHz βιομηχανική, επιστημονική και ιατρική ζώνη (ISM- Industrial, Scientific and Medical Band), όπως πολλές άλλες ασύρματες τεχνολογίες. Χρησιμοποιεί την τοπολογία πλέγματος, βασιζόμενο στο φυσικό επίπεδο του πρωτοκόλλου IEEE 802.15.4 και προσθέτει το επίπεδο ζεύξης δεδομένων, το επίπεδο δικτύου, το επίπεδο μεταφοράς και το επίπεδο εφαρμογής [99, 100]. Βασίζεται στην τεχνολογία πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA), η οποία είναι διαλειτουργική με τους τύπους ασύρματων συσκευών διαφόρων κατασκευαστών. Όλες οι συσκευές είναι χρονικά συγχρονισμένες και επικοινωνούν μέσα σε προκαθορισμένες χρονοθυρίδες. Το TDMA ελαχιστοποιεί τις συγκρούσεις και μειώνει την κατανάλωση ισχύος των συσκευών [99], [102]. Τα βασικά συστατικά ενός WirelessHART δικτύου είναι τα εξής [102]:

- Οι Συσκευές Πεδίου (Field Devices)
- Οι Προσαρμογείς (Adapters)
- Ο Δρομολογητής (Router)
- Η Πύλη (Gateway)
- Οι Συσκευές χειρός (Handheld Devices)

- Ο Διαχειριστής Δικτύου (Network Manager)
- Ο Διαχειριστής Ασφαλείας (Security manager)

Η στοίβα πρωτοκόλλων του προτύπου WirelessHART βασίζεται στην αρχιτεκτονική επιπέδων του OSI.

- Το φυσικό στρώμα βασίζεται στο πρωτόκολλο IEEE 802.15.4 και λειτουργεί στις συχνότητες που καθορίζονται από αυτό, δηλαδή στα 2,4 GHz της ζώνης ISM
- Το επίπεδο ζεύξης δεδομένων υιοθετεί την τεχνική της χρονικής πολυπλεξίας (TDMA) και κάνει χρήση των superframes για την αποφυγή συγκρούσεων κατά την διάρκεια της επικοινωνίας
- Το επίπεδο δικτύου είναι υπεύθυνο για την δρομολόγηση των πακέτων από την πηγή προς τον τελικό προορισμό, συντηρεί τους πίνακες δρομολόγησης και παρέχει ασφάλεια στις επικοινωνίες από άκρο σε άκρο. [99]
- Το επίπεδο μεταφοράς είναι υπεύθυνο για την μεταφορά του πακέτου από άκρο σε άκρο σε διάφορες συσκευές εντός δικτύου [99]
- Το επίπεδο εφαρμογής είναι στην ουσία το πρότυπο HART. Παρέχει πρόσβαση στο πρότυπο WirelessHART μέσω των κεντρικών υπολογιστικών συστημάτων, των φορητών υπολογιστών και των συστημάτων διαχείρισης [104]

NeuRFon

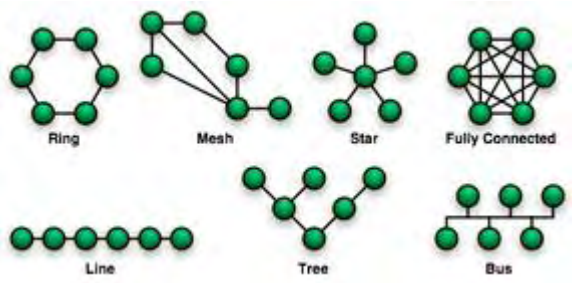
Το NeuRFon οφείλει το όνομα του στις λέξεις νευρώνας (neuron) κα ραδιοεκπομπή (RF). Ήταν ένα ερευνητικό πρόγραμμα που ξεκίνησε το 1999 στη Motorola Labs για την ανάπτυξη ad hoc δικτύων σε εφαρμογές ασύρματων δικτύων αισθητήρων. Η βιολογική αναλογία είναι ότι, οι μεμονωμένοι νευρώνες δεν είναι πολύ χρήσιμοι ενώ ένα μεγάλο δίκτυο το οποίο αποτελείται από πολλούς νευρώνες είναι πολύ ισχυρό. Η ίδια ιδέα ισχύει και για τα δίκτυα αισθητήρων, τα οποία αποτελούνται από πολλές, απλές, ασύρματες συσκευές χαμηλής ισχύος. Μεγάλο μέρος της τεχνολογίας που αναπτύχθηκε στο πλαίσιο του προγράμματος NeuRFon ενσωματώθηκε στο πρότυπο IEEE 802.15.4 και στις προδιαγραφές του ZigBee. Παραδείγματα είναι ο καθορισμός του φυσικού επίπεδου στα 2.4 GHz και σημαντικό μέρος του πρωτοκόλλου δρομολόγησης πολλαπλών αλμάτων του ZigBee. [77], [78]

2.1.3 Τοπολογίες Δικτύου

Ως τοπολογία δικτύου, ορίζεται η διάταξη των διαφόρων στοιχείων των τηλεπικοινωνιακών δικτύων όπως οι συνδέσεις, οι κόμβοι κ.α. Αποτελεί την αναπαράσταση ενός δικτύου και μπορεί να απεικονιστεί *φυσικά* ή *λογικά*. Η **φυσική τοπολογία** απεικονίζει τις θέσεις των στοιχείων του δικτύου (συσκευές, καλώδια, κλπ) όπως θα ήταν στο χώρο. Συγκεκριμένα, αναφέρεται στη διάταξη των καλωδίων, στις θέσεις των κόμβων, στις αποστάσεις που καλύπτουν και στους συνδέσμους μεταξύ των κόμβων και της καλωδίωσης.

Η **λογική τοπολογία** ή **τοπολογία σήματος** παρουσιάζει την ροή των δεδομένων μέσα στο δίκτυο. Αφορά στην ηλεκτρονική και προγραμματιστική πραγματοποίηση της επικοινωνίας. Δεν ενδιαφέρεται για την ισχύ του σήματος όταν αυτό διαδίδεται μέσα σε ένα σύστημα.

Ενδιαφέρεται για τον τρόπο και την λογική της διάδοσης του σήματος ανεξάρτητα με την φυσική διασύνδεση των συσκευών, και τον τρόπο που περνούν τα δεδομένα από το ένα σημείο του δικτύου στο άλλο, ακόμα και αν αυτό αφορά το εσωτερικό μιας δικτυακής συσκευής. Η διαφορετική χρήση των δύο τοπολογιών έχει σαν αποτέλεσμα πολλές φορές στο ίδιο δίκτυο να διαφέρει η φυσική από την λογική τοπολογία. [148]

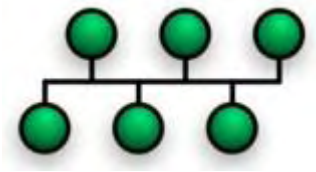


Διάγραμμα διαφορετικών τοπολογιών δικτύων [148]

Η διάταξη των στοιχείων ενός δικτύου μπορεί να ταξινομηθεί στις παρακάτω βασικές τοπολογίες:

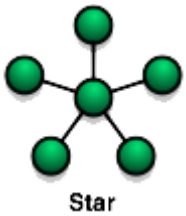
Η **δισημειακή τοπολογία** (**point-to-point topology**) είναι η απλούστερη τοπολογία και είναι μια μόνιμη σύνδεση μεταξύ δύο σημείων. Είναι η σύνδεση που επιτρέπει ανεμπόδιστη επικοινωνία μεταξύ δύο σημείων. Χαρακτηριστικό παράδειγμα είναι η σύνδεση των δικτύων σε απομακρυσμένα υποκαταστήματα μιας εταιρείας μέσω αποκλειστικών τηλεφωνικών κυκλωμάτων.

Η **τοπολογία διαύλου** (**bus topology**), στην οποία κάθε κόμβος συνδέεται σε ένα κεντρικό καλώδιο. Αυτό το κεντρικό καλώδιο είναι ο κορμός (backbone ή bus) του δικτύου και είναι γνωστό ως δίαυλος ή αρτηρία. Ένα πακέτο δεδομένων που έχει αφετηρία έναν από τους κόμβους ταξιδεύει και στις δύο κατευθύνσεις και διαδοχικά διέρχεται από όλους τους άλλους κόμβους του διαύλου. Δεδομένου ότι τα πακέτα διασχίζουν όλο το δίκτυο ανεξάρτητα της θέσης του κόμβου-αποδέκτη ενδέχεται να επιβαρύνουν την συνολική του απόδοση. Η συγκεκριμένη τοπολογία είναι ακατάλληλη για μεγάλα δίκτυα. [148]



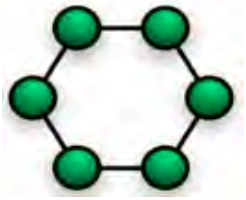
Τοπολογία διαύλου [148]

Η **τοπολογία αστέρα** (**star topology**), στην οποία κάθε κόμβος (συσκευή) είναι συνδεδεμένος σε ένα "κεντρικό" κόμβο. Σε αυτή την τοπολογία ένα πακέτο δεδομένων που έχει αφετηρία έναν από τους περιφερειακούς κόμβους κατευθύνεται πάντα στον κεντρικό κόμβο ο οποίος το αναμεταδίδει σε όλους τους κόμβους. Οι περιφερειακοί κόμβοι επικοινωνούν μεταξύ τους με αποστολές και λήψεις στον κεντρικό κόμβο. Όπως και στην *τοπολογία διαύλου* η απόδοση του δικτύου επιβαρύνεται λόγω της μεταφοράς πακέτων σε όλους τους κόμβους. Το δίκτυο γίνεται πιο αποτελεσματικό όταν ο κεντρικός κόμβος είναι μεταγωγέας (switch). Ο μεταγωγέας διαβάζει την διεύθυνση παραλήπτη του πακέτου και το στέλνει αποκλειστικά στον κόμβο-αποδέκτη [148]



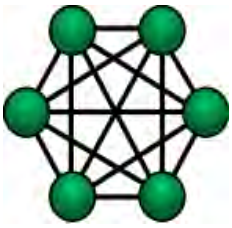
Τοπολογία Αστέρα [148]

Η **τοπολογία δακτυλίου** (**ring topology**) είναι σαν την τοπολογία διαύλου (bus) στην οποία όμως τα δύο άκρα ενώνονται σε έναν κλειστό βρόχο. Τα δεδομένα διαδίδονται προς μία κατεύθυνση, αν και υπάρχουν δακτύλιοι διπλής κατεύθυνσης. Πλεονεκτεί της τοπολογίας αστέρα στο ότι δεν χρειάζεται τον "κεντρικό" κόμβο. Μειονέκτημα είναι ότι αν μια από τις συνδέσεις μεταξύ των κόμβων έχει μικρότερη ταχύτητα μεταφοράς δεδομένων καθυστερεί ολόκληρο το δίκτυο. [148]



Τοπολογία δακτυλίου [148]

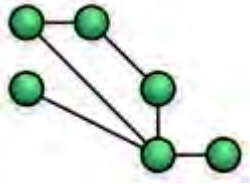
Η **κατανεμημένη τοπολογία** (**mesh topology**) στην οποία, όλοι οι κόμβοι (συσκευές) του δικτύου συνδέονται μεταξύ τους μερικά ή στο σύνολό τους, έτσι ώστε να μην κατατάσσονται σε κάποια από τις προηγούμενες τοπολογίες. Διακρίνουμε :
Την **Πλήρως κατανεμημένη τοπολογία** (fully connected topology ή fully connected mesh topology) όλοι οι κόμβοι συνδέονται μεταξύ τους. Ο αριθμός των συνδέσεων (connections) αυξάνεται τετραγωνικά σε σχέση με τον αριθμό των κόμβων (nodes). Δηλαδή $\boldsymbol{connections} = \frac{\boldsymbol{nodes(nodes-1)}}{\boldsymbol{2}}$, που για δίκτυα με πολλούς κόμβους είναι περίπου $\frac{\boldsymbol{nodes^2}}{\boldsymbol{2}}$**.** Η τοπολογία αυτή δεν έχει πρακτική εφαρμογή στα μεγάλα δίκτυα. [148]



Πλήρως κατανεμημένη τοπολογία [148]

Την **Μερικώς κατανεμημένη τοπολογία** (Partially connected mesh topology) στην οποία κάποιοι κόμβοι έχουν περισσότερες από μια συνδέσεις με τους άλλους κόμβους του δικτύου. Σε μια τέτοια τοπολογία δύο απομακρυσμένοι κόμβοι μπορούν να επικοινωνούν ακολουθώντας μια διαδρομή ενδιάμεσων κόμβων. Σε αυτή την περίπτωση αν κάποια από τις συνδέσεις του τεθεί εκτός λειτουργίας ή για κάποιο λόγο μειωθεί ο ρυθμός μετάδοσης, υπάρχει η δυνατότητα εναλλακτικών διαδρομών. Αυτό προϋποθέτει την ύπαρξη κατάλληλων αλγόριθμων που θα

καθορίζουν την βέλτιστη διαδρομή δρομολόγησης (routing) ανάλογα με την κάθε περίσταση. [148]



Μερικώς κατανεμημένη τοπολογία [148]

2.1.4 Θέματα Ασφάλειας

Η έννοια της ασφάλειας ενός ασύρματου δικτύου αισθητήρων σχετίζεται με την ικανότητα της προστασίας των πληροφοριών του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητα του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στις εξουσιοδοτημένες οντότητες όταν τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου [105]. Αν και η ασφάλεια στα δίκτυα υπολογιστών είναι μια καλά εδραιωμένη επιστημονική περιοχή, με πρωτόκολλα και πρότυπα τα οποία τυγχάνουν ευρείας αναγνώρισης, η προσαρμογή και χρησιμοποίηση αυτών στα δίκτυα ασυρμάτων αισθητήρων είναι τις περισσότερες φορές, αν όχι αδύνατη, πάρα πολύ δύσκολη, εξαιτίας των ιδιαίτερων χαρακτηριστικών των δικτύων αισθητήρων τόσο εξαιτίας των περιορισμών των κόμβων που τα απαρτίζουν, όσο και εξαιτίας των ιδιαίτερων χαρακτηριστικών των εφαρμογών στις οποίες χρησιμοποιούνται.

Επειδή τα δίκτυα αισθητήρων τις περισσότερες φορές αναπτύσσονται σε περιβάλλοντα στα οποία δεν μπορεί να γίνει εύκολα η συντήρηση του δικτύου, είναι αναγκαίο να λάβουμε μέριμνα ώστε το δίκτυο να γνωρίζει τις πιθανές απειλές καθώς επίσης και τους μηχανισμούς ώστε να προστατευτεί από τις επιθέσεις. Οι απειλές που δέχεται ένας κόμβος του δικτύου μπορούν να χωριστούν, στις **επιθέσεις** και στην **κακή συμπεριφορά** [107].

Σαν «επίθεση» ορίζουμε οποιαδήποτε πράξη που σκόπιμα προσπαθεί να προκαλέσει ζημιά στο δίκτυο. Σαν απειλές κακής συμπεριφοράς ορίζονται οι αυθαίρετες συμπεριφορές εσωτερικών κόμβων που μπορούν να οδηγήσουν αθέλητα σε καταστροφή άλλων κόμβων. Ο στόχος του κόμβου δεν είναι να επιτεθεί σε έναν άλλο κόμβο, αλλά μπορεί να έχει άλλους στόχους, όπως να αποκτήσει ένα άδικο πλεονέκτημα σε σύγκριση με άλλους κόμβους. Για παράδειγμα, ένας κόμβος μπορεί να μην εκτελέσει σωστά το πρωτόκολλο MAC με σκοπό να λάβει μεγαλύτερο εύρος ζώνης ή μπορεί να αρνηθεί να προωθήσει πακέτα για άλλους για να μην καταναλώσει κομμάτι της ενέργειάς του, ενώ χρησιμοποιεί την ενέργειά του και ζητά από άλλους κόμβους να προωθούν τα δικά του πακέτα.

Σχετικά με την ασφάλεια, θα πρέπει να τονίσουμε πως αποτελεί ίσως το σημαντικότερο κομμάτι κατά τη δημιουργία και ανάπτυξη ενός ασύρματου δικτύου. Για τον λόγο αυτό πρέπει κατά την σχεδίαση να ληφθεί μέριμνα ώστε το ασύρματο δίκτυο να μπορεί να αντιμετωπίσει ένα πλήθος πιθανών επιθέσεων ανάλογα πάντα με τις απαιτήσεις, τις ιδιαιτερότητες και τις τεχνικές προδιαγραφές της εκάστοτε εφαρμογής. Για την αντιμετώπιση των απειλών ένα ασύρματο δίκτυο

πρέπει να μπορεί να τηρεί τις αρχές ασφαλείας. Οι σημαντικότερες απαιτήσεις ασφαλείας περιγράφονται παρακάτω [105]:

- Διαθεσιμότητα
- Εμπιστευτικότητα
- Ακεραιότητα
- Αυθεντικότητα [109-111]
- Μη αποποίηση [108]
- Φρεσκάδα πληροφοριών[109][110]

Παρακάτω περιγράφονται τα κενά ασφαλείας όπως προκύπτουν από τα ιδιαίτερα χαρακτηριστικά των ασύρματων δικτύων αισθητήρων [106],[110],[114]:

Περιορισμοί κόστους: οι κόμβοι του δικτύου πρέπει να είναι περιορισμένης οικονομικής αξίας, διαφορετικά λόγω του μεγάλου αριθμού τους στο δίκτυο, η εφαρμογή μπορεί να είναι οικονομικά ασύμφορη. Αποτέλεσμα είναι κάθε κόμβος να έχει περιορισμένη ισχύ επεξεργασίας και χώρο αποθήκευσης δεδομένων.

Ενέργεια: τα ασύρματα δίκτυα αισθητήρων λειτουργούν με μπαταρία ή με κάποιο άλλο αυτόνομο μέσο. Πρέπει λοιπόν οι μηχανισμοί ασφαλείας να μην είναι ενεργοβόροι. Επίσης οι επιθέσεις στον κόμβο μπορούν να εστιάσουν στην κατανάλωση ενέργειας του, ώστε να βγει εκτός λειτουργίας.

Ασύρματες συνδέσεις: η ανταλλαγή μηνυμάτων μεταξύ των κόμβων μπορεί να υποκλαπεί από οποιονδήποτε έχει τοποθετήσει ένα δέκτη στην περιοχή. Επιπλέον τα σήματα είναι συνήθως χαμηλής ενέργειας με αποτέλεσμα να ευνοούνται ενδεχόμενες επιθέσεις με ισχυρούς πομπούς.

Περιοχή: πολλές φορές η περιοχή όπου αναπτύσσεται το ασύρματο δίκτυο αισθητήρων είναι εύκολα προσβάσιμη για αυτόν του πραγματοποιεί την επίθεση.

Τοπολογία δικτύου: τα δίκτυα αισθητήρων συνήθως χρησιμοποιούν επικοινωνία πολλαπλών αλμάτων με τοπολογία πλέγματος. Τα δεδομένα λοιπόν θα περάσουν από αρκετούς κόμβους μέχρι να φτάσουν στον τελικό στόχο.

Μέγεθος πακέτου: τα σήματα από τους αισθητήρες απαιτούν ένα μικρό μέγεθος δεδομένων για να περιγραφούν. Επιπλέον με την αποστολή μικρού μεγέθους πακέτων επιτυγχάνεται εξοικονόμησης ενέργειας. Οι μηχανισμοί ασφαλείας που θα εφαρμοστούν δεν πρέπει να αυξάνουν κατά πολύ το μέγεθος του πακέτου δεδομένων.

Κινητικότητα: σε αρκετές εφαρμογές οι κόμβοι μετακινούνται. Η κίνηση αυτή μπορεί να είναι εντός του δικτύου, αλλά και εκτός του δικτύου με επιστροφή σε απρόβλεπτη χρονική στιγμή. Οι μηχανισμοί ασφαλείας πρέπει να λαμβάνουν μέριμνα για πιθανή κινητικότητα των κόμβων, η οποία δεν είναι προκαθορισμένη.

Έλλειψη υποδομής: τα ιδιαίτερα χαρακτηριστικά των δικτύων αισθητήρων δεν ευνοούν την ύπαρξη κεντρικής διαχείρισης αλλά τείνουν σε κατανεμημένα σχήματα. Οι μηχανισμοί ασφαλείας πρέπει να στηρίζονται σε κατανεμημένα συνεργατικά σχήματα και όχι σε κεντρικά σχήματα ασφαλείας.

2.1.5 Παραδείγματα WSN Εφαρμογών

Η ασύρματη δικτύωση και η δυνατότητα αυτό-οργάνωσης των ασύρματων δικτύων αισθητήρων χωρίς την ανάγκη ανθρώπινης παρέμβασης, κάνει δυνατή την εξάπλωση τους σε περιβάλλοντα που είναι δύσκολο ή ακόμη και αδύνατο να πάει ο άνθρωπος, όπως τα περιβάλλοντα φυσικών πόρων. Η έλλειψη καλωδίωσης για την επίτευξη της μεταξύ τους επικοινωνίας έχει ως αποτέλεσμα να μπορούμε να παρατηρούμε το φαινόμενο από μεγάλη ή ασφαλή απόσταση. [119]

Σημαντική επίσης υπήρξε και η χρήση τους για τον εντοπισμό συμβάντων ή θέσης, όπως σεισμικών δραστηριοτήτων ή κινούμενων αντικειμένων, γεγονός που εισήγαγε την έννοια του εντοπισμού συμβάντος ως μια επιπλέον δυνατότητα στη χρήση των δικτύων αυτών. Μια τρίτη εφαρμογή των δικτύων αυτών, η ανίχνευση καταστάσεων, κινείται κάπου μεταξύ της παρακολούθησης, συλλογής δεδομένων και του εντοπισμού συμβάντος. Μπορούμε να κατατάξουμε τα ασύρματα δίκτυα αισθητήρων σε δυο βασικές κατηγορίες [117][118]:

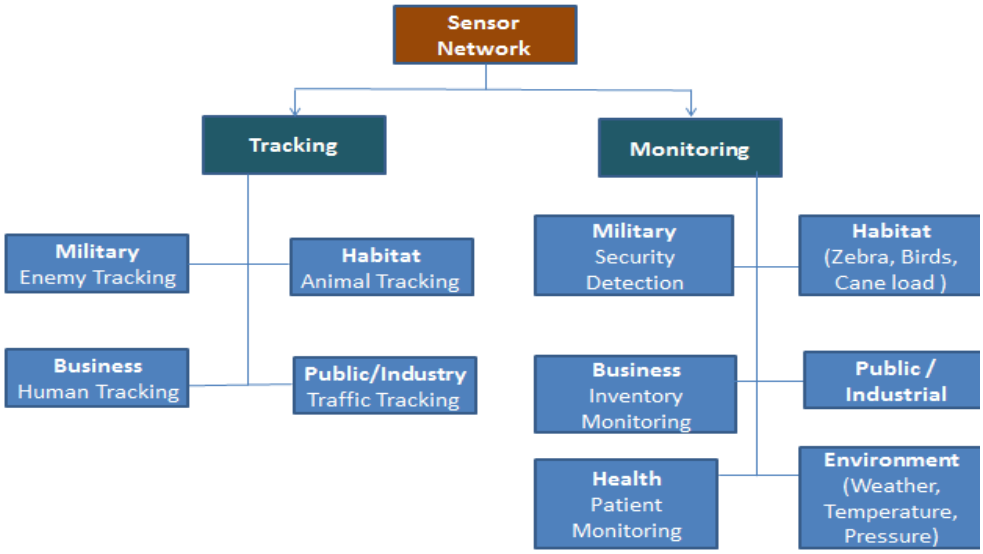
- της επίβλεψης (monitoring)
- της ανίχνευσης (tracking)

Αυτές με την σειρά τους μπορούν να χωριστούν σε:

- Παρακολούθηση χώρου
- Παρακολούθηση αντικειμένων
- Παρατήρηση της αλληλεπίδρασης των αντικειμένων και περιβάλλοντος χώρου

Ενδεικτικά, ορισμένες εφαρμογές αναφέρονται ακολούθως [119]:

- Περιβαλλοντικές εφαρμογές
- Γεωργικές εφαρμογές [117]
- Εφαρμογές πρόληψης καταστροφών και παροχής βοήθειας
- Οικιακές εφαρμογές
- Επιτήρηση μηχανών και βιομηχανικές εφαρμογές
- Επιτήρηση αντικειμένων
- Εφαρμογές ασφαλείας
- Στρατιωτικές εφαρμογές
- Τηλεματική - έλεγχος μεταφορών και συγκοινωνιών
- Ιατρικές εφαρμογές και Υγιεινή [132-134]
- Άλλες εμπορικές εφαρμογές

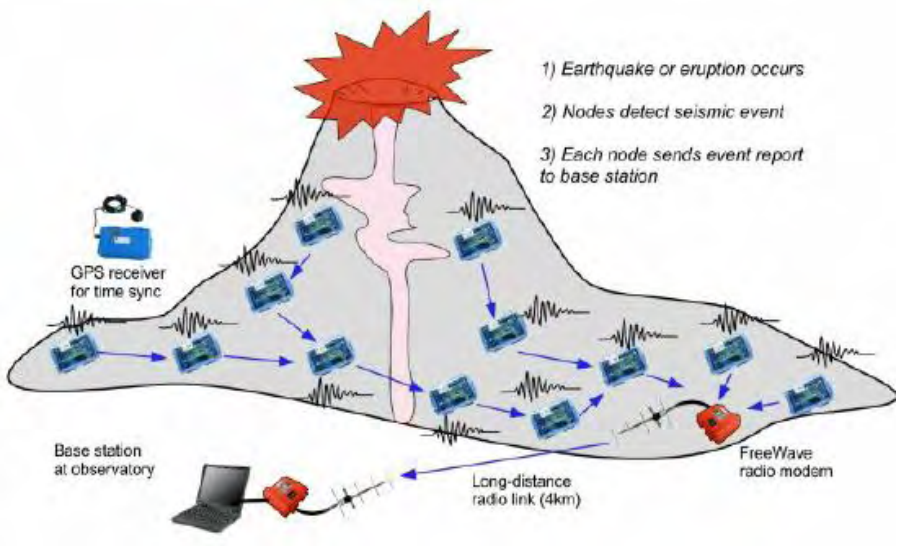


Εφαρμογές των WSN [115]

Περιβαλλοντικές εφαρμογές

Σήμερα υπάρχει ένας μεγάλος αριθμός περιβαλλοντολογικών εφαρμογών ασύρματων δικτύων αισθητήρων για τη καταγραφή της εξελικτικής διαδικασίας ενός οικοσυστήματος υδάτινου, χερσαίου, δασικού ή αστικού. Στις εφαρμογές αυτές χρησιμοποιούνται συνήθως αισθητήρες βροχόπτωσης, στάθμης νερού και αισθητήρες καιρού για μετεωρολογική, γεωφυσική έρευνα και μελέτη της ρύπανσης. Επίσης υπάρχουν εφαρμογές για την ρύθμιση των κλιματικών συνθηκών στα μεγάλα κτήρια ώστε να εξασφαλίσει ένα περιβάλλον εργασίας υγιές και ευχάριστο.
[117], [120], [121]

Εφαρμογές ασύρματων δικτύων αισθητήρων υλοποιήθηκαν ακόμα και σε ακραία περιβάλλοντα, όπου η συνεχής ανθρώπινη πρόσβαση είναι αδύνατη. Η παρακολούθηση ηφαιστείου είναι ένα παράδειγμα αυτών των ακραίων εφαρμογών, όπου ένα δίκτυο αισθητήρων μπορεί εύκολα να αναπτυχθεί κοντά σε ενεργό ηφαίστειο και να παρακολουθεί συνεχώς τις δραστηριότητες παρέχοντας πληροφόρηση που με τα μέχρι πρότινος εργαλεία δεν ήταν εφικτή. Δυο τέτοιες εφαρμογές έλαβαν χώρο σε δυο ηφαίστεια του Εκουαδόρ κατά την περίοδο 2004-2005.[120], [123]



Παρακολούθηση ηφαιστειακής δραστηριότητας με χρήση WSN [116]

Εφαρμογές πρόληψης καταστροφών και παροχής βοήθειας

Τα ασύρματα δίκτυα αισθητήρων μπορούν να βρουν εφαρμογή σε μια σειρά από επείγουσες καταστάσεις εποπτεύοντας περιοχές με αυξημένο κίνδυνο εκδήλωσης κάποιας καταστροφής. Τυπικές εφαρμογές είναι η πυρανίχνευση, ο έλεγχος πλημυρών και ο έλεγχος τεχνικών κατασκευών.[117], [120], [127]

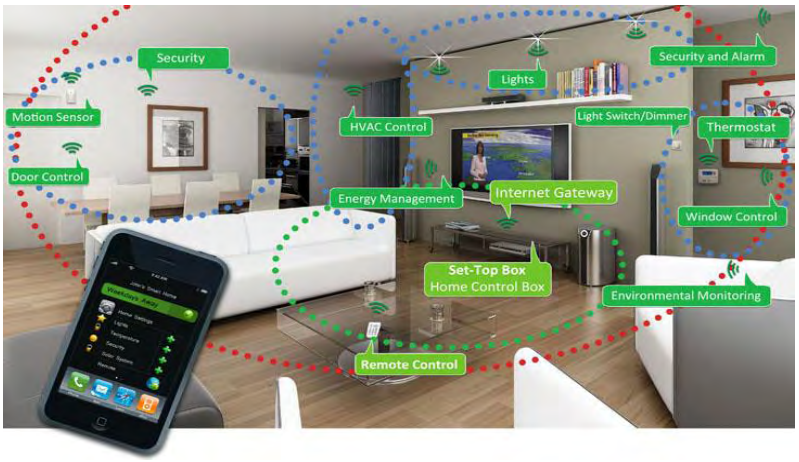
Ανάλογα με το πιθανό αίτιο πρόκλησης μίας πλημμύρας σε κάποια συγκεκριμένη γεωγραφική περιοχή, μπορεί να εγκατασταθεί σε αυτήν ένα ασύρματο δίκτυο αισθητήρων για την έγκαιρη ανίχνευση κι αντιμετώπιση της. Ένα παράδειγμα συστήματος ανίχνευσης πλημμύρων είναι το σύστημα ALERT, το οποίο και αναπτύχθηκε στις ΗΠΑ. Στο σύστημα αυτό χρησιμοποιήθηκαν διάφοροι τύποι αισθητήρων, όπως μέτρησης της στάθμης της βροχόπτωσης, της θερμοκρασίας, της υγρασίας και της στάθμης του νερού. Τα δεδομένα από αυτές τις μετρήσεις αποστέλλονται σε μια ή περισσότερες κεντρικές αποθήκες δεδομένων, όπου και υφίστανται επεξεργασία για την αποτελεσματική πρόληψη, καθώς και την αντιμετώπιση των πλημμύρων [117].

Οικιακές εφαρμογές

Από τις εφαρμογές των ασύρματων δικτύων αισθητήρων δεν θα μπορούσαν να εκλείψουν οι οικιστικές εφαρμογές. Στις εφαρμογές για οικιακή χρήση, τα ασύρματα δίκτυα αισθητήρων συμβάλλουν στην προώθηση των οικιακών αυτοματισμών, στην υλοποίηση έξυπνων σπιτιών με περιβάλλοντα που προσαρμόζονται ανάλογα με τις εξωτερικές συνθήκες ή τις επιλογές του χρήστη. Στόχος είναι η μείωση της σπατάλης σε ενέργεια με τον έλεγχο της υγρασίας, του εξαερισμού και του κλιματισμού (humidity, ventilation, air-conditioning- HVAC). Έτσι όχι μόνο πετυχαίνεται η εξοικονόμηση ενέργειας αλλά βελτιώνεται και το βιοτικό επίπεδο των κατοίκων. [117][120].

Στην περίπτωση των «έξυπνων» σπιτιών γίνεται χρήση ασύρματων αισθητήρων σε μεμονωμένα αντικείμενα καθημερινής και ευρείας χρήσης. Με τον τρόπο αυτό

παρακολουθούνται οι όποιες δραστηριότητες του χώρου και των μεταβολών που υφίστανται τα αντικείμενα αυτά οι οποίες οφείλονται σε ανθρώπινη χειραγώγηση. [129], [130]



Χρήση WSN για παρακολούθηση «έξυπνου σπιτιού» [130]

2.2 Τεχνολογίες IoT

2.2.1 Smart "things"

Το Διαδίκτυο των πραγμάτων (IoT) και των πρωτοκόλλων του αποτελούν ένα από τα πιο υψηλά χρηματοδοτούμενα θέματα τόσο στη βιομηχανία όσο και στην πανεπιστημιακή κοινότητα. Η ταχύτατη εξέλιξη του mobile internet, του mini- hardware manufacturing, του micro-computing, και της M2M επικοινωνίας, άνοιξαν τον δρόμο για την εδραίωση του IoT. Σύμφωνα με την Gartner, το IoT κυριαρχεί αυτή τη στιγμή στο hype-cycle* της, το οποίο σημαίνει αναπόφευκτα ότι το IoT είναι κορυφαίο στις επενδύσεις στον τομέα της βιομηχανίας, αναφερόμενη στα δισεκατομμύρια που ξοδεύονται αυτή τη στιγμή γύρω από τις τεχνολογίες και την έρευνα. [136]

Οι IoT τεχνολογίες επιτρέπουν σε πράγματα ή συσκευές που δεν είναι υπολογιστές, να ενεργούν έξυπνα και να παίρνουν συλλογικές αποφάσεις που είναι ωφέλιμες σε συγκεκριμένες χρήσεις. Επιπλέον, επιτρέπουν στα πράγματα να «ακούνε», να «βλέπουν», να «σκέφτονται» ή να «δρουν» σε συνδυασμό με το να επικοινωνούν και να συντονίζονται μέσω εντολών ώστε να παίρνουν αποφάσεις οι οποίες μπορεί να είναι τόσο καθοριστικές και κρίσιμες όσο να σώζουν μια ανθρώπινη ζωή ή ένα κτήριο. Μετατρέπουν τα πράγματα από παθητικά αντικείμενα που αποφασίζουν ατομικά σε «έξυπνα» αντικείμενα που παίρνουν κρίσιμες αποφάσεις δρώντας συλλογικά και όντας παντού παρόντα. Οι θεμέλιες τεχνολογίες της πανταχού παρούσης υπολογιστικής, των ενσωματωμένων αισθητήρων, των επικοινωνιών ορατού φωτός και των πρωτοκόλλων του Ίντερνετ ανέδειξαν τη σπουδαιότητα του IoT αλλά επίσης επέβαλλαν πολλές προκλήσεις για την ανάπτυξη εξειδικευμένων προτύπων και πρωτοκόλλων επικοινωνίας.

2.2.2 IoT πρωτόκολλα πρόσβασης (Thread, Zigbee, Z-Wave, Bluetooth-Le)

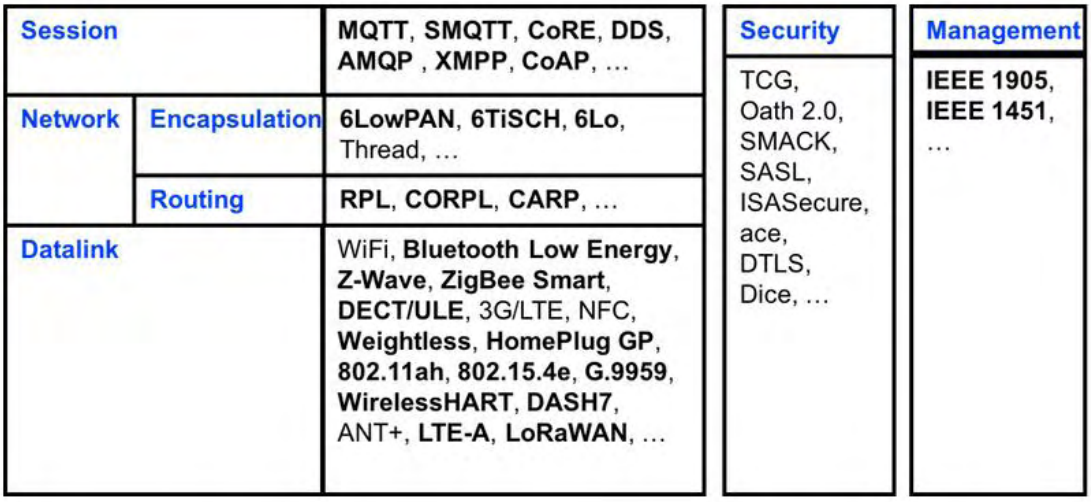
Σε αυτό το κεφάλαιο, επισημαίνονται πρωτόκολλα που λειτουργούν σε διαφορετικά επίπεδα της στοίβας του δικτύου, περιλαμβάνοντας: το επίπεδο Ζεύξης δεδομένων, το επίπεδο Δικτύου και το επίπεδο Συνόδου. Παρουσιάζονται επίσης πρότυπα όπως προσφέρονται από το Internet Engineering Task Force (IETF), το Institute of Electrical and Electronics Engineers (IEEE), το International Telecommunication Union (ITU) και από άλλους οργανισμούς. Αυτά τα πρότυπα έχουν προταθεί την τελευταία δεκαετία ώστε να καλύπτουν τις τωρινές αλλά και τις μελλοντικές ανάγκες του IoT. [137]

Το παρακάτω σχήμα δείχνει ένα μοντέλο 7-επιπέδων του IoT οικοσυστήματος (IoT ecosystem). Στη βάση του μοντέλου βρίσκεται η αγορά ή ο τομέας εφαρμογών ο οποίος μπορεί να είναι ένα έξυπνο ηλεκτρικό δίκτυο, ένα έξυπνο σπίτι κλπ. Το δεύτερο επίπεδο αποτελείται από αισθητήρες που ενεργοποιούν την εφαρμογή. Παραδείγματα τέτοιων αισθητήρων είναι οι αισθητήρες θερμοκρασίας, υγρασίας, κάμερες κ.α. Το τρίτο επίπεδο είναι το επίπεδο διασύνδεσης το οποίο επιτρέπει στα δεδομένα που παράγονται από τους αισθητήρες να επικοινωνήσουν συνήθως με ένα κέντρο δεδομένων ή με ένα αποθηκευτικό νέφος (cloud). Εκεί, τα δεδομένα συγκεντρώνονται με άλλες ομάδες δεδομένων όπως γεωγραφικά, πληθυσμιακά ή οικονομικά δεδομένα. Ο συνδυασμός των παραπάνω δεδομένων στη συνέχεια αναλύεται χρησιμοποιώντας μηχανική μάθηση και τεχνικές εξόρυξης δεδομένων. Για να είναι δυνατόν να λάβουν μέρος τόσο μεγάλα διανεμημένες εφαρμογές, χρειαζόμαστε επίσης το τελευταίο λογισμικό συνεργασίας και επικοινωνίας επιπέδου εφαρμογής όπως το software defined networking (SDN), services oriented architecture (SOA), κ.α. Τέλος, η κορυφή των επιπέδων αποτελείται από υπηρεσίες που ενεργοποιούν την αγορά και μπορεί να περιλαμβάνουν διαχείριση ενέργειας, διαχείριση υγείας, εκπαίδευση, μέσα μεταφοράς κ.α. Πέραν των 7 αυτών επιπέδων που είναι χτισμένα ώστε να αλληλοεξαρτώνται, υπάρχουν εφαρμογές διοίκησης και ασφάλειας για το κάθε επίπεδο, οι οποίες φαίνονται στο πλάι.

Το οικοσύστημα του IoT [137]

Το επίπεδο διασύνδεσης (Interconnection Layer) του οικοσυστήματος του IoT μπορεί να αναλυθεί σε περαιτέρω διαστρωμάτωση όπως φαίνεται στην παρακάτω εικόνα. Τα επίπεδα αυτά είναι το επίπεδο ζεύξης δεδομένων, το επίπεδο δικτύου και το συνενωμένο επίπεδο μεταφοράς/συνόδου. Το επίπεδο ζεύξης δεδομένων συνδέει δύο IoT στοιχεία όπως δύο

αισθητήρες ή τον αισθητήρα με την πύλη δικτύου που συνδέει όλους τους αισθητήρες με το Ίντερνετ. Συχνά, υπάρχει η ανάγκη για αρκετούς αισθητήρες να επικοινωνούν και να συγκεντρώνουν τις πληροφορίες πριν να βγουν στο Ίντερνετ. Γι αυτό το λόγο, ειδικά πρωτόκολλα έχουν σχεδιαστεί για τη δρομολόγηση μεταξύ των αισθητήρων και ανήκουν στο επίπεδο δρομολόγησης. Τα πρωτόκολλα που ανήκουν στο επίπεδο συνόδου, είναι υπεύθυνα για τα μηνύματα που ανταλλάσσουν όλα τα IoT στοιχεία. Τέλος, έχουν αναπτυχθεί και πρωτόκολλα ασφαλείας και διαχείρισης για το IoT όπως φαίνονται στην ίδια εικόνα.



Πρωτόκολλα του IoT [137]

Τα πρωτόκολλα του επιπέδου ζεύξης δεδομένων περιλαμβάνουν τα πρωτόκολλα των physical και MAC επιπέδων τα οποία συνδυάζονται στα περισσότερα πρότυπα.

ZigBee [84-91]

Το ZigBee αποτελεί επέκταση της στοίβας πρωτοκόλλων του 802.15.4, όπως είδαμε νωρίτερα, καθώς υλοποιεί τα επίπεδα δικτύου και εφαρμογών, βασιζόμενο στις υπηρεσίες που παρέχουν το φυσικό επίπεδο και το MAC υπο-επίπεδο του 802.15.4. Η ZigBee Alliance είναι μια κοινή ομάδα πολλών μεγάλων εταιρειών, η οποία ανέπτυξε το πρωτόκολλο ZigBee ως ένα πρότυπο χαμηλού κόστους και πολύ χαμηλής κατανάλωσης, αμφίδρομης και ασύρματης επικοινωνίας.

Το IEEE 802.15.4 επικεντρώνεται στα δύο χαμηλότερα επίπεδα της στοίβας του πρωτοκόλλου, ενώ το ZigBee συγκεντρώνεται στην παροχή των πιο υψηλών επιπέδων για τη λειτουργικότητα των δεδομένων δικτύωσης και για υπηρεσίες ασφαλείας. Το πρωτόκολλο ZigBee υποστηρίζει τις τρεις βασικές τοπολογίες του IEEE 802.15.4. Τα βασικά χαρακτηριστικά του είναι ο χαμηλός ρυθμός μετάδοσης δεδομένων, η δυνατότητα να υποστηρίξει μέχρι 254 συσκευές σε τοπολογία αστέρα και η γρήγορη επαναφορά των συσκευών από κατάσταση sleep. Το δίκτυο ZigBee είναι πολλαπλής πρόσβασης, αφού όλες οι συσκευές έχουν ισότιμη πρόσβαση στο μέσο επικοινωνίας. Υπάρχουν δύο τύποι μηχανισμών πολλαπλής πρόσβασης:

- Ο μηχανισμός με λειτουργία beacon, όπου οι συσκευές επιτρέπεται να εκπέμπουν μόνο σε προκαθορισμένες χρονοθυρίδες, και

- Η λειτουργία non-beacon, στην οποία όλες οι συσκευές μπορούν να εκπέμψουν οποιαδήποτε χρονική στιγμή, εφόσον το κανάλι είναι ελεύθερο.

Η στοίβα πρωτοκόλλων του ZigBee βρίσκεται στο πάνω μέρος του φυσικού επιπέδου και του MAC υπο-επιπέδου, που έχουν καθοριστεί από το πρότυπο IEEE 802.15.4.
Η στοίβα πρωτοκόλλων ορίζει τα ακόλουθα επίπεδα:

1. Το Επίπεδο Δικτύου- ZigBee Network Layer (NWK)

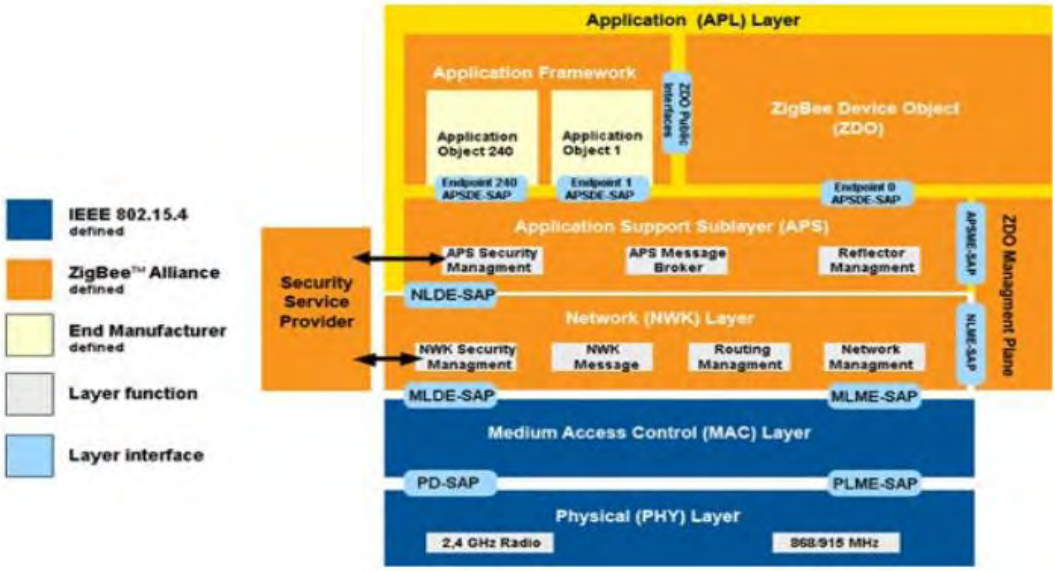
Το NWK επίπεδο αποτελεί τη γέφυρα μεταξύ των δύο προτύπων, του 802.15.4 και του ZigBee, καθώς εξασφαλίζει τη σωστή λειτουργία του MAC υπο-επιπέδου και είναι υπεύθυνο για την οργάνωση και την παροχή δρομολόγησης σε ένα multi-hop δίκτυο, που βασίζεται στη λειτουργία του IEEE 802.15.4.

2. Το Επίπεδο Εφαρμογής- ZigBee Application Layer (APL)

Το επίπεδο αυτό είναι το υψηλότερο και το πολυπλοκότερο που ορίζει το πρότυπο και προσφέρει μια δομή για την ανάπτυξη και την επικοινωνία κατανεμημένων εφαρμογών. Αποτελείται από τα Αντικείμενα Εφαρμογών (Application Objects), το Αντικείμενο Συσκευής ZigBee (ZigBee Application Object) και το υπο-επίπεδο Υποστήριξης Εφαρμογής (Application Support SubLayer - APS).

3. Το Πλαίσιο Εργασίας Εφαρμογών- ZigBee Application Framework (AF)

Το επίπεδο AF είναι το τελευταίο επίπεδο του πρωτοκόλλου ZigBee και είναι υπεύθυνο για την ύπαρξη και τη διαμονή όλων των αντικειμένων της εφαρμογής στο δίκτυο.



Αρχιτεκτονική της στοίβας ZigBee και IEEE 802.15.4 [83]

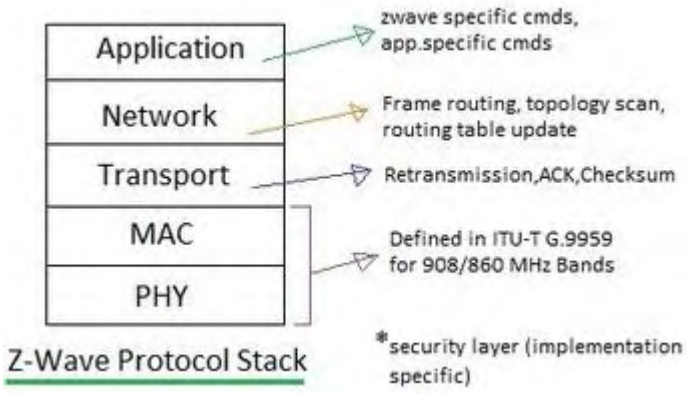
Z-Wave [142]

Το Z-Wave είναι ένα χαμηλής ισχύος MAC πρωτόκολλο που έχει σχεδιαστεί για αυτοματισμούς κατοικιών και χρησιμοποιείται για IoT επικοινωνία, ειδικά σε έξυπνα σπίτια και σε μικρούς εμπορικούς τομείς από τη συμμαχία Z-Wave. Το Z-Wave παρέχει τη δυνατότητα κάλυψης έως 30 μέτρων επικοινωνίας point-to-point και είναι κατάλληλο για μικρά μηνύματα σε IoT εφαρμογές, όπως για έλεγχο φωτισμού, έλεγχο ενέργειας, έλεγχο της υγείας μέσω φορητών συσκευών (wearables) κ.α. Χρησιμοποιεί CSMA/CA για ανίχνευση συγκρούσεων και ACK

μηνύματα για αξιόπιστη μετάδοση δεδομένων. Το Z-Wave λειτουργεί στη ζώνη ISM για την ενιαία συχνότητα χρησιμοποιώντας τη μέθοδο μετατόπισης συχνότητας (FSK). Η ρυθμαπόδοση είναι 40 kbps και είναι κατάλληλο για εφαρμογές ελέγχου και αισθητήρες. Κάθε δίκτυο Z-Wave μπορεί να περιλαμβάνει μέχρι 232 κόμβους. Η αρχιτεκτονική που ακολουθεί είναι το μοντέλο master/slave, όπου ο master έχει τον έλεγχο των slaves, τους στέλνει εντολές και χειρίζεται τον προγραμματισμό του όλου δικτύου. [139]

Ένας από τους στόχους του Z-Wave ήταν να προσφέρει ένα απλοποιημένο ασύρματο πρωτόκολλο που θα μεταφέρει αξιόπιστα μηνύματα σε μια κατοικία. Η στοίβα Z-Wave αποτελείται από (εικόνα τάδε) :

- Το φυσικό στρώμα/στρώμα MAC για έλεγχο της πρόσβασης στο μέσο RF
- Το στρώμα μεταφοράς που χειρίζεται ελέγχους ακεραιότητας πλαισίου, αναγνωρίσεις, και αναμεταδόσεις.
- Ένα στρώμα δικτύου που χειρίζεται την δρομολόγηση των πλαισίων και παρέχει διεπαφές εφαρμογών.



Στοίβα πρωτοκόλλου Z-Wave [142]

Υπάρχουν δύο κύριοι τύποι συσκευών που ορίζονται στο πρωτόκολλο Z-Wave όπως ήδη αναφέραμε: οι ελεγκτές-masters και οι συσκευές σκλάβοι-slaves. Οι ελεγκτές είναι σε θέση να ξεκινήσουν μια μετάδοση καθώς και να κρατήσουν όλα τα στοιχεία που σχετίζονται με τις δρομολογήσεις του δικτύου. Οι συσκευές σκλάβοι, από την άλλη πλευρά, είναι απλά συσκευές γενικού σκοπού με λειτουργικότητα τύπου εισόδου-εξόδου (GPIO) που εκτελούν τυφλά τα αιτήματα του ελεγκτή.

Η διαχείριση των κόμβων στο Z-Wave αποτελείται από δύο κύριες λειτουργίες, ένταξη/αποκλεισμός και συσχέτιση. Η ένταξη εγκαινιάζει ένα νέο κόμβο στο δίκτυο. Το αντίστροφο είναι ο αποκλεισμός, το οποίο περιγράφει τη διαδικασία για την απομάκρυνση ενός κόμβου. Η συσχέτιση είναι η δημιουργία της λογικής σύνδεσης μεταξύ των συσκευών.

Bluetooth Low Energy

Το Bluetooth Low Energy είναι ένα πρότυπο δικτύωσης συσκευών χαμηλής κατανάλωσης και χαμηλού χρόνου αναμονής, σε δίκτυα μικρής εμβέλειας (έως 50 μέτρα). Αρχικά, η ιδέα του Bluetooth LE γεννήθηκε από την Nokia το 2001 ως ένα ερευνητικό πρόγραμμα, έπειτα από την διαπίστωση ότι υπάρχουν κάποια σοβαρά προβλήματα στην

κατανάλωση ενέργειας που με την υπάρχουσα τεχνολογία δικτύωσης ήταν ανέφικτο να λυθούν. Το 2009, παρουσιάστηκε το νέο Bluetooth LE ως μια επιπρόσθετη στοίβα πρωτοκόλλου στο πρότυπο Bluetooth 4.0, συμβατή με άλλες υπάρχουσες στοίβες πρωτοκόλλων. [94],[98]

Η χαμηλή του ενέργεια είναι ως και 10 φορές λιγότερη από το κλασικό Bluetooth ενώ παράλληλα η καθυστέρηση μεταφοράς (latency) μπορεί να γίνει μέχρι και 15 φορές μικρότερη. Ακολουθεί την αρχιτεκτονική master/slave και παρέχει πλαίσια (frames) δύο ειδών: advertising και data. Το advertising frame χρησιμοποιείται για ανακάλυψη και στέλνεται από τους slaves μέσω ενός ή περισσότερων ειδικών διαφημιστικών καναλιών. Οι κόμβοι masters, ψάχνουν στα διαφημιστικά κανάλια να βρουν slaves και να επικοινωνήσουν μαζί τους. Μετά την σύνδεση τους, ο master ενημερώνει τον slave για τον κύκλο εγρήγορσης (waking cycle) και την ακολουθία προγραμματισμού (scheduling sequence). Οι κόμβοι είναι στην κατάσταση awake μόνο όταν επικοινωνούν και επιστρέφουν στην κατάσταση sleep αμέσως μετά για εξοικονόμηση ενέργειας [140],[141]. Περιπτώσεις χρήσης του Bluetooth LE περιλαμβάνουν αισθητήρες στο χώρο του αθλητισμού, της ιατρικής, της ασφάλειας καθώς και της οικιακής ψυχαγωγίας. [98]

Υπάρχουν δυο βασικοί τύποι συστημάτων ασύρματης τεχνολογίας Bluetooth οι οποίοι και είναι οι:

- Βασικού ρυθμού (Basic Rate – BR)
- Χαμηλής ενέργειας (Low Energy– LE)

Η τεχνολογία του Bluetooth LE είναι προσανατολισμένη σε γνωρίσματα που έχουν σχεδιαστεί για προϊόντα που απαιτούν μικρότερη κατανάλωση ισχύος, έχουν μικρότερη πολυπλοκότητα και χαμηλότερο κόστος καθώς επίσης για περιπτώσεις χρήσης και εφαρμογές χαμηλότερου ρυθμού δεδομένων. [92-97].

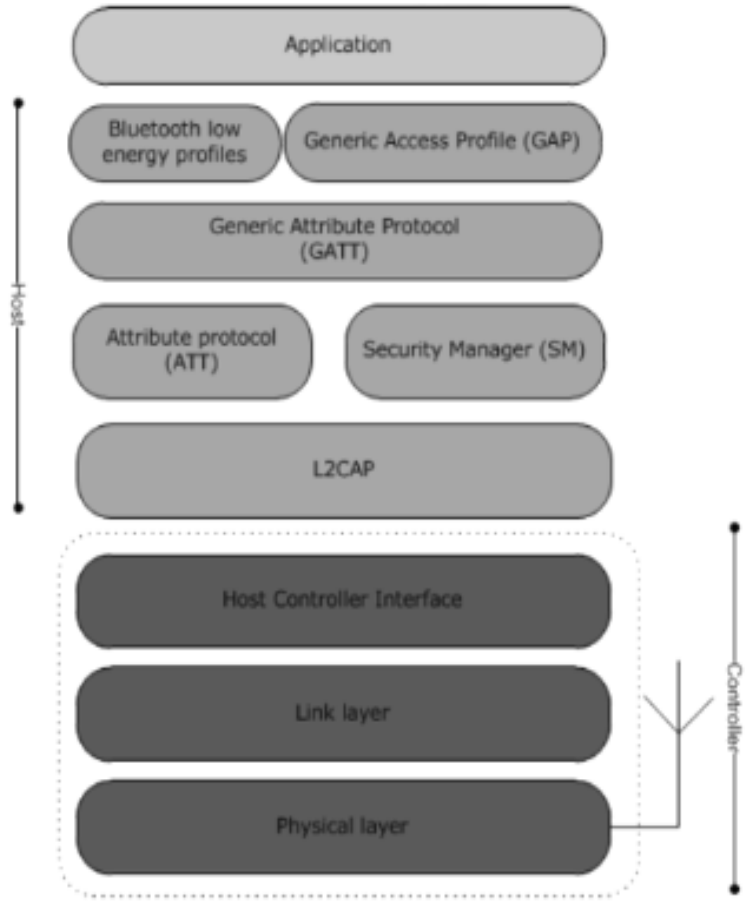
Το Bluetooth LE λειτουργεί στη ελεύθερη ζώνη συχνοτήτων των 2.4 GHz. Χρησιμοποιεί έναν πομποδέκτη αναπήδησης συχνότητας για την αντιμετώπιση παρεμβολών και εξασθένησης και παρέχει πολλούς φορείς FHSS. Ο πυρήνας της τεχνολογίας Bluetooth LE χωρίζεται στον **host** και στον **ελεγκτή** (controller). Ο host του πυρήνα Bluetooth LE αποτελείται από:

- Τον διαχειριστή καναλιού (Channel manager)
- Τον διαχειριστή πόρων L2CAP (L2CAP resource manager)
- Το πρωτόκολλο διαχείρισης ασφάλειας(Security Manager Protocol-SMP)
- Το πρωτόκολλο ιδιοχαρακτηριστικών (Attribute Protocol-ATT)
- Τον διαχειριστή AMP (AMP Manager)
- Το γενικό προφίλ ιδιοχαρακτηριστικών (Generic Attribute Protocol-GATT)
- Το γενικό προφίλ πρόσβασης (Generic Access Profile-GAP)

Ενώ στον ελεγκτή, σε υλοποιήσεις όπου συνδυάζονται συστήματα BR/EDR και LE, τα αρχιτεκτονικά μπλοκ μπορούν να μοιράζονται ανάμεσα στα συστήματα ή κάθε σύστημα μπορεί να έχει ξεχωριστή αρχιτεκτονική αποτελούμενη από:

- Τον διαχειριστή συσκευής (Device Manager)
- Τον διαχειριστή ζεύξης (Link Manager)
- Τον διαχειριστή πόρων ζώνης βάσης (Baseband Resource Manager)
- Τον ελεγκτή ζεύξης (Link Controller)
- Το φυσικό επίπεδο (Physical Layer - PHY)

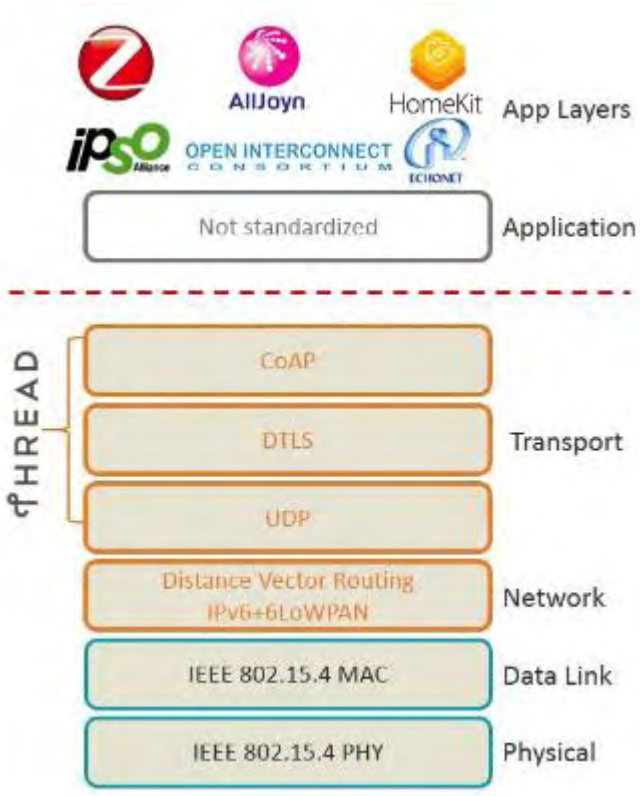
[93]



Αρχιτεκτονική Bluetooth LE [92]

Thread

Το Thread είναι ένα μια IPv6-βασιζόμενη, χαμηλής ισχύος ασύρματη τεχνολογία πλέγματος που χρησιμοποιείται σε IoT προϊόντα και σχεδιάστηκε για να είναι ασφαλής και διαχρονική. Η στοίβα πρωτοκόλλων Thread αποτελεί ένα ελεύθερο πρότυπο που βασίζεται σε μια συλλογή από ήδη υπάρχοντα IEEE και IETF πρότυπα και δεν αποτελεί ένα καινούργιο εξ' ολοκλήρου πρότυπο. [144]



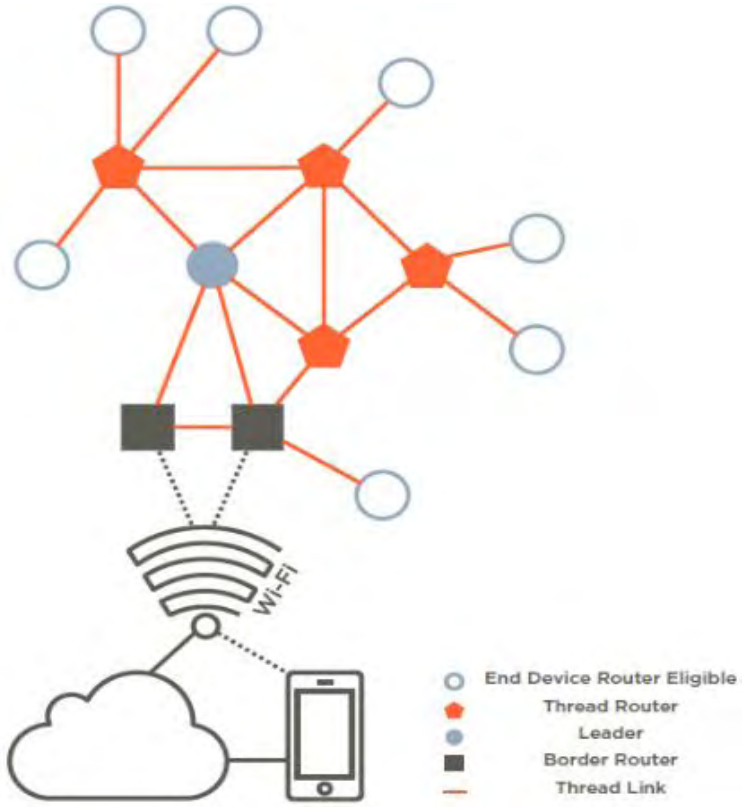
Η στοίβα πρωτοκόλλων του Thread [144]

Η στοίβα πρωτοκόλλων του Thread υποστηρίζει IPv6 διευθυνσιοδότηση, παρέχει χαμηλού κόστους σύνδεση (bridging) με άλλα IP δίκτυα και προσφέρεται για χαμηλής ισχύος ασύρματη M2M επικοινωνία. Σχεδιάστηκε ειδικά για εφαρμογές ενός διασυνδεδεμένου σπιτιού και παρακάτω παρουσιάζονται τα κύρια χαρακτηριστικά της στοίβας πρωτοκόλλων με εστίαση στο διασυνδεδεμένο σπίτι:

- Απλή εγκατάσταση του δικτύου, έναρξη και λειτουργία: Η στοίβα πρωτοκόλλων υποστηρίζει αρκετές τοπολογίες. Η εγκατάσταση είναι απλή με τη χρήση ενός smartphone, tablet ή υπολογιστή.
- Ασφάλεια: Οι συσκευές δεν μπορούν να μπουν στο δίκτυο εκτός κι αν έχουν εξουσιοδότηση καθώς και όλες οι επικοινωνίες είναι ασφαλείς και με κρυπτογράφηση. Όλα τα Thread δίκτυα είναι κρυπτογραφημένα χρησιμοποιώντας έναν μηχανισμό αυθεντικοποίησης smartphone-era καθώς και κρυπτογράφηση AES.
- Μικρά και μεγάλα δίκτυα: Τα οικιακά δίκτυα χρησιμοποιούν από αρκετές μέχρι εκατοντάδες συσκευές. Το επίπεδο δικτύου της τεχνολογίας Thread σχεδιάστηκε ώστε να αξιοποιεί τη λειτουργία του δικτύου ανάλογα με τις απαιτούμενες ανάγκες.
- Εύρος: Οι τυπικές συσκευές παρέχουν επαρκές εύρος για να καλύψουν ένα κανονικό σπίτι, όμως οι πρόθυμα διαθέσιμες συσκευές με ενισχυτές, με την τεχνολογία Thread, μπορούν να αυξάνουν το εύρος κάλυψης σημαντικά και αποτελεσματικά
- Χωρίς «αστοχία ενός και μόνο σημείου»: Η στοίβα πρωτοκόλλων Thread έχει σχεδιαστεί για να παρέχει ασφάλεια και αξιόπιστο χειρισμό ακόμη και αν υπάρξει απώλεια ή αποτυχία κάποιας μεμονωμένης συσκευής.

- Χαμηλή ισχύς: Οι συσκευές επικοινωνούν με αποδοτικότητα, παρέχουν βελτιωμένη εμπειρία χρήστη και κάτω από κανονικές συνθήκες χρήσης μπαταρίας τύπου AA έχουν μεγάλη διάρκεια ζωής.
- Οικονομικά-αποδοτικό: Συμβατά chipset και λογισμικό από πολλούς πωλητές τιμολογούνται για μαζική χρήση και σχεδιάζονται από το μηδέν ώστε να έχουν χαμηλή κατανάλωση ενέργειας.

Οι χρήστες ενός δικτύου Thread επικοινωνούν από την προσωπική τους συσκευή (smartphone, tablet, υπολογιστής) μέσω του Wi-Fi του οικιακού τους δικτύου ή χρησιμοποιώντας μια πλατφόρμα υπολογιστικού νέφους. Το παρακάτω σχήμα παρουσιάζει τα βασικά είδη συσκευών της αρχιτεκτονικής ενός δικτύου Thread. [144]



Αρχιτεκτονική δικτύου Thread [144]

Τα παρακάτω είδη συσκευών περιλαμβάνονται σε ένα δίκτυο Thread. Ξεκινώντας από το ασύρματο δίκτυο έχουμε:

Border routers, οι οποίοι παρέχουν τη συνδεσιμότητα από το 802.15.4 δίκτυο σε γειτονικά δίκτυα άλλων φυσικών επιπέδων (Wi-Fi, Ethernet, κ.α) και αναλαμβάνουν υπηρεσίες δρομολόγησης και εκτός του δικτύου τους. **Leader**, ο οποίος διαχειρίζεται το μητρώο των router IDs που έχουν μοιραστεί και δέχεται αιτήματα από συσκευές router-eligible end devices (REEDs) που θέλουν να γίνουν δρομολογητές. **Thread routers,** οι οποίοι παρέχουν υπηρεσίες δρομολόγησης στις συσκευές του δικτύου αλλά και υπηρεσίες ασφάλειας σύνδεσης για όσες συσκευές επιχειρούν να εισέλθουν στο δίκτυο. **REEDs,** οι οποίοι μπορούν να γίνουν thread routers ή leader, αλλά όχι απαραίτητα border routers διότι οι τελευταίοι έχουν ειδικές ιδιότητες

όπως πολλαπλά interface. **End devices** οι οποίες δεν είναι υποψήφιοι δρομολογητές αλλά μπορούν να είναι FEDs (full end devices) ή MEDs (minimal end devices). **Sleepy end devices,** οι οποίες επικοινωνούν μόνο μέσω του thread «γονιού» τους και δεν υποστηρίζουν αποστολή μηνυμάτων προς άλλες συσκευές.

Όλες οι συσκευές χρησιμοποιούν το 6LoWPAN όπως αυτό ορίζεται στο RFC 4944. Ο σκοπός του 6LoWPAN είναι να λάβει και να μεταδώσει IPv6 πακέτα μέσω των 802.15.4 συνδέσεων. Σε μια τέτοια σύνδεση, το 6LoWPAN δρα ως μέσο προσαρμογής μεταξύ του IPv6 δικτύου και του data link επιπέδου του 802.15.4. [144]

Τέλος οι συσκευές Thread υποστηρίζουν το πρωτόκολλο ICMPv6, τα ICMPv6 error messages, echo request και echo reply messages όπως επίσης και το πρωτόκολλο UDP για αποστολή μηνυμάτων μεταξύ των συσκευών.

Όσον αφορά την τοπολογία ενός Thread δικτύου, αυτή εξαρτάται από τον αριθμό των δρομολογητών που συμμετέχουν στο δίκτυο. Εάν υπάρχει μόνο ένας δρομολογητής στο δίκτυο τότε το δίκτυο είναι τύπου αστέρα (star), ενώ αν υπάρχουν περισσότεροι δρομολογητές, τότε αυτόματα δημιουργείται ένα κατανεμημένο δίκτυο ή αλλιώς τύπου πλέγματος (mesh).

Σχετικά με τη δρομολόγηση δεδομένων στο Thread δίκτυο, αυτή είναι τύπου next hop και βασίζεται στον πίνακα δρομολόγησης που διατηρείται από τη στοίβα και εγγυάται ότι όλοι οι δρομολογητές θα έχουν συνδεσιμότητα και ενημερωμένες διαδρομές για όλους τους δρομολογητές του δικτύου. Όλοι οι δρομολογητές του δικτύου ανταλλάσσουν μεταξύ τους τα κόστη για την κάθε διαδρομή τους προς τους άλλους δρομολογητές σε συμπιεσμένο format χρησιμοποιώντας το πρωτόκολλο MLE. [144]

Τέλος, όσον αφορά στην ασφάλεια του Thread δικτύου, όντας ασύρματο θα πρέπει να είναι ασφαλές από over-the-air (OTA) επιθέσεις κι επειδή θα είναι και συνδεδεμένο στο Ίντερνετ, θα πρέπει να είναι ασφαλές και από τις επιθέσεις του. Το Thread χρησιμοποιεί ένα ειδικό κλειδί (network-wide key) για κρυπτογράφηση που πραγματοποιείται στο επίπεδο MAC. Αυτό το κλειδί χρησιμοποιείται για αυθεντικοποίηση και κρυπτογράφηση του προτύπου IEEE 802.15.4-2006 και προστατεύει το Thread δίκτυο από over-the-air επιθέσεις που ξεκινούν από εξωτερικά δίκτυα. Το δίκτυο Thread επιτρέπει στο επίπεδο εφαρμογής να εφαρμόζει οποιοδήποτε πρωτόκολλο διαδικτύου για ασφάλεια στην από άκρο σε άκρο επικοινωνία. [144]

2.2.3 Τεχνολογίες Υποδομής (Infrastructure Technologies) [149]

«Το IoT απαιτεί ένα εκτενές εύρος από νέες τεχνολογίες και επιδεξιότητες που ακόμη αρκετές εταιρείες δεν έχουν τελειοποιήσει. Ένα επαναλαμβανόμενο μοτίβο στο χώρο του IoT είναι η ανωριμότητα των υπαρχόντων τεχνολογιών και υπηρεσιών και των πωλητών που τις παρέχουν», ανέφερε ο Nick Jones, αντιπρόεδρος και διακεκριμένος αναλυτής της Gartner. Οι κορυφαίες δέκα IoT τεχνολογίες για το 2017 και το 2018 είναι οι εξής:

IoT Security: Οι τεχνολογίες ασφαλείας θα κληθούν να προστατέψουν τις IoT συσκευές και πλατφόρμες από επιθέσεις και αλλοιώσεις των δεδομένων και των πληροφοριών του IoT συστήματος, να κρυπτογραφήσουν την επικοινωνία τους και να εισάγουν νέες προκλήσεις έναντι της μιμήσεως των «πραγμάτων» του IoT και των επιθέσεων άρνησης-της-κατάστασης-sleep που έχουν ως στόχο την εξάντληση των μπαταριών των έξυπνων συσκευών. Η ασφάλεια στο IoT θα είναι αρκετά περίπλοκη διαδικασίας καθώς αρκετά «πράγματα» του IoT χρησιμοποιούν απλούς

επεξεργαστές με απλό λειτουργικό σύστημα που πιθανώς να μην υποστηρίζουν πολύπλοκες τεχνικές ασφαλείας.

IoT Analytics. Τα επαγγελματικά μοντέλα του IoT θα εκμεταλλευτούν την πληροφορία που συλλέγεται από τα «πράγματα» του IoT με πολλούς τρόπους. Για παράδειγμα, για την κατανόηση της συμπεριφοράς του καταναλωτή, για να βελτιώσουν προϊόντα και υπηρεσίες και για να αναγνωρίζουν και να ανακόπτουν τα «business moments» (κατά Gartner.

IoT Device (Thing) Management. Τα μακρόβια και διόλου ευκαταφρόνητα «πράγματα» του IoT θα έχουν την ανάγκη διαχείρισης και παρακολούθησης. Αυτό περιλαμβάνει παρακολούθηση συσκευών, ενημέρωση του υλικολογισμικού (firmware) και του λογισμικού, διαγνωστικά, crash analysis κ.α.

Short range low-power IoT Networks. Η επιλογή ενός ασύρματου δικτύου για μια IoT συσκευή περιλαμβάνει την εξισορρόπηση πολλών αντικρουόμενων απαιτήσεων, όπως το εύρος, τη διάρκεια ζωής της μπαταρίας, το bandwidth, την πυκνότητα ισχύος κ.α. Τα χαμηλής ενέργειας και μικρής εμβέλειας IoT δίκτυα κυριάρχησαν στην ασύρματη συνδεσιμότητα του IoT μέχρι το 2015, υπερέχοντας αριθμητικά από συνδέσεις ευρείας περιοχής.

Low-Power Wide Area Networks (LPWAN). Ο μακροπρόθεσμος στόχος ενός δικτύου ευρείας περιοχής είναι να πετυχαίνει ρυθμούς μετάδοσης δεδομένων από εκατοντάδες bps σε δεκάδες kbps με δυνατότητα εθνικής κάλυψης, διάρκεια ζωής μπαταρίας πάνω από 10 χρόνια, πολύ χαμηλό κόστος τερματικού και να υποστηρίζει εκατοντάδες χιλιάδες συσκευές συνδεδεμένες σε ένα σταθμό βάσης. Το πρότυπο Narrowband IoT (NB-IoT), πιθανώς θα κυριαρχήσει σε αυτό το χώρο.

IoT processors. Οι επεξεργαστές και οι αρχιτεκτονικές που χρησιμοποιούνται από τις συσκευές του IoT καθορίζουν πολλές από τις ικανότητες τους, όπως αν είναι ικανές για ισχυρή ασφάλεια και κρυπτογράφηση, την κατανάλωση ισχύος, αν είναι αρκετά εξελιγμένες και σύγχρονες ώστε να υποστηρίζουν ένα λειτουργικό σύστημα, δυνατότητα αναβάθμισης του υλικολογισμικού και πράκτορες διαχείρισης ενσωματωμένους στη συσκευή. Ως αποτέλεσμα, η κατανόηση των συνεπειών της επιλογής των επεξεργαστών θα απαιτεί πολύ τεχνικές δεξιότητες.

IoT Operating Systems. Τα παραδοσιακά λειτουργικά συστήματα όπως τα Windows και τα iOS δεν έχουν σχεδιαστεί για IoT εφαρμογές. Καταναλώνουν υπερβολική ενέργεια, χρειάζονται γρήγορους επεξεργαστές και σε κάποιες περιπτώσεις, υστερούν λειτουργιών. Γι αυτόν τον λόγο, μεγάλος αριθμός λειτουργικών συστημάτων ειδικά για IoT έχουν αναπτυχθεί για να ανταπεξέλθουν στις παραπάνω ανάγκες.

Event Stream Processing. Μερικές IoT εφαρμογές θα παράγουν υπερβολικά υψηλούς ρυθμούς δεδομένων που θα πρέπει να αναλύονται σε πραγματικό χρόνο. Για να αντιμετωπιστούν αυτές οι απαιτήσεις, χρησιμοποιούνται κατανεμημένες υπολογιστικές πλατφόρμες ροής-distributed stream computing platforms (DSCPs) που χρησιμοποιούν παράλληλες αρχιτεκτονικές για να επεξεργαστούν δεδομένα πολύ υψηλού ρυθμού μεταφοράς ώστε να εκτελούν διεργασίες όπως η αναλυτική πραγματικού χρόνου και η αναγνώριση μοτίβων.

IoT platforms. Οι IoT πλατφόρμες συνδυάζουν πολλά δομικά στοιχεία της υποδομής ενός IoT συστήματος σε ένα προϊόν. Οι υπηρεσίες που παρέχουν αυτές οι πλατφόρμες χωρίζονται σε τρεις βασικές κατηγορίες: (1) έλεγχος συσκευής και λειτουργιών χαμηλού επιπέδου, (2) απόκτηση, μετατροπή και διαχείριση IoT δεδομένων και (3) ανάπτυξη της IoT εφαρμογής που περιλαμβάνει προγραμματισμό της εφαρμογής, απεικόνιση, αναλυτική και προσαρμογείς για σύνδεση στο σύστημα της επιχείρησης.

IoT Standards and Ecosystems. Τα πρότυπα και τα αντίστοιχα API τους θα είναι αναγκαία γιατί οι IoT συσκευές θα χρειάζεται να επικοινωνούν και να διαλειτουργούν και αρκετά επιχειρησιακά IoT μοντέλα θα βασίζονται στον καταμερισμό των δεδομένων μεταξύ συσκευών και οργανισμών. Οι οργανισμοί θα πρέπει να καταφέρουν να υποστηρίξουν τα διαφορετικά πρότυπα ή οικοσυστήματα και να είναι έτοιμοι να αναβαθμίσουν τα προϊόντα τους κατά τη διάρκεια ζωής τους.

Περισσότερη ανάλυση μπορεί να βρει κανείς στην αναφορά της Gartner για το Internet of Things με τίτλο "Top 10 IoT Technologies for 2017 and 2018." [149]

2.2.4 Θέματα Ασφάλειας σε IoT Εφαρμογές

Η ασφάλεια είναι ένα ακόμη σημαντικό θέμα που αφορά τις IoT εφαρμογές καθώς απειλές μπορεί να βρεθούν σχεδόν σε όλα τα επίπεδα των IoT πρωτοκόλλων. Όλο και περισσότερες συσκευές και αντικείμενα καθημερινής χρήσης έχουν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων σχετικά με το περιβάλλον γύρω τους και τα άτομα που τα χρησιμοποιούν. Ενώ το IoT υπόσχεται πως μέσω αυτών των δεδομένων θα ενισχύσει την άνεση και την αποτελεσματικότητα στις διάφορες καθημερινές λειτουργίες, εντούτοις, η συλλογή τους εμπεριέχει σημαντικές επιπτώσεις στην ιδιωτική ζωή και την προστασία της.

Ούτε στην Ευρώπη αλλά ούτε και στις ΗΠΑ δεν υπάρχει ακόμα καθορισμένο νομικό πλαίσιο που να επιβάλλει την προστασία του τεράστιου όγκου προσωπικών δεδομένων που συλλέγονται μέσω των διαφόρων συσκευών, ούτε να αναγκάζει τους κατασκευαστές των συσκευών αυτών να υιοθετούν ικανοποιητικά πρωτόκολλα ασφαλείας. Εναπόκειται στη διακριτική ευχέρεια του κάθε κατασκευαστή κατά πόσον θα λάβει οποιεσδήποτε ενέργειες προς αυτή την κατεύθυνση.

Η βασική λειτουργία του IoT, δηλαδή η διασύνδεση πολλαπλών καθημερινών αντικειμένων μέσω του διαδικτύου, γεννά αρκετούς προβληματισμούς. Αν τα «πράγματα» αυτά συνδέονται στο διαδίκτυο, τότε ποιος μπορεί να δει τα δεδομένα τους και ποιος να τα ελέγξει; Μπορεί οποιοσδήποτε να μάθει για την κατανάλωση ενέργειας ενός σπιτιού; Πού καταλήγουν τα προσωπικά δεδομένα και ποιός εγγυάται για την ασφάλεια τους; Ποιός ελέγχει και διασφαλίζει την τήρηση όλων των παραπάνω και γενικά το IoT και τη βιομηχανία του; Τα ερωτήματα αυτά μπορούν να ομαδοποιηθούν στις εξής τρείς κατηγορίες:

Θέματα ελέγχου πρόσβασης- Ο έλεγχος πρόσβασης έχει ως σκοπό να διαχειριστεί την αλληλεπίδραση και την επικοινωνία μεταξύ χρηστών και συστημάτων. Ένα κανάλι ασφαλούς επικοινωνίας, είναι αποτέλεσμα συνήθως μιας επιτυχημένης διαδικασίας πιστοποίησης.

Θέματα απορρήτου και ασφαλείας- Ένα από τα μεγαλύτερα προβλήματα ασφαλείας που δημιουργείται με τη χρήση των IoT συσκευών είναι το πώς χρησιμοποιούνται τα δεδομένα που συλλέγουν από το περιβάλλον του χρήστη. Στην περίπτωση των επιχειρήσεων και των οργανισμών, μπορεί να εκτεθεί η παραγωγική τους διαδικασία και να γίνουν θύματα βιομηχανικής κατασκοπείας. Φυσικά, χωρίς την συλλογή αυτών των δεδομένων η ύπαρξη των έξυπνων συσκευών δεν θα είχε καμία αξία αφού δεν θα παρείχαν καμία διευκόλυνση στον χρήστη. Ο προβληματισμός έγκειται στον τρόπο που χρησιμοποιούνται, από ποιους και με ποιον απώτερο σκοπό. [158]

Θέματα πολιτικής και νομοθεσίας- Η μεγαλύτερη πρόκληση στον τομέα του IoT είναι η σύμπλευση τους με το Νόμο. Το πρώτο μεγάλο βήμα της Ε.Ε προς της κατεύθυνση της προστασίας των προσωπικών δεδομένων ήταν η Οδηγία 95/46/ΕΚ, η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Νόμο 2472/1997 που μετρούσε ήδη 20 έτη εφαρμογής. Η ανάγκη για προσαρμογή της νομοθεσίας στις σύγχρονες τεχνολογικές συνθήκες κατεύθυναν την Ε.Ε στην ψήφιση του **Κανονισμού 2016/679** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την **κατάργηση της Οδηγίας 95/46/ΕΚ**.

Ο Κανονισμός αυτός που τέθηκε σε εφαρμογή στις 25 Μαΐου 2018, προσφέρει πλούσια νομική βάση για ζητήματα που αφορούν το IoT. Καθοριστικής σημασίας για την προστασία των δεδομένων αποτελούν, το άρθρο 3 για το πεδίο γεωγραφικής εφαρμογής, το άρθρο 7 αναφορικά με τις προϋποθέσεις συγκατάθεσης, το άρθρο 12 για το δικαίωμα ενημέρωσης και το άρθρο 17 για το θεμελιώδες δικαίωμα στη λήθη (right to be forgotten).

Τα προβλήματα που θα αντιμετωπίσουν οι κατασκευαστές-προμηθευτές IoT, στην περίπτωση που αγνοήσουν τις εφαρμογές ιδιωτικότητας και προστασίας προσωπικών δεδομένων είναι αρκετά και σε πολλές περιπτώσεις μπορεί γίνουν καταστροφικά. Για παραβίαση συγκεκριμένων άρθρων του Κανονισμού τα πρόστιμα φτάνουν έως 20.000.000 ευρώ και αν πρόκειται για επιχειρήσεις, το 4% του συνολικού παγκόσμιου ετήσιου τζίρου του προηγούμενου οικονομικού έτους. [159]

2.2.5 CoAP και MQTT

Το **Constrained Application Protocol (CoAP)** είναι ένα συγχρονισμένο πρωτόκολλο επιπέδου συνόδου και τύπου πελάτη-εξυπηρετητή το οποίο σχεδιάστηκε από το Internet Engineering Task Force (IETF), παρόμοιο με το HTTP και προορίζεται για συσκευές με περιορισμένους πόρους.[153] Οι περισσότερες συσκευές που χρησιμοποιούνται σε ένα WSN έχουν περιορισμένη χωρητικότητα σε μνήμη RAM καθώς και περιορισμένες δυνατότητες επεξεργασίας δεδομένων. Οι συσκευές αυτές συνήθως συνδέονται σε δίκτυα με χαμηλό εύρος ζώνης, όπως το 6LoWPAN, τα οποία έχουν υψηλό ποσοστό απώλειας πακέτων. Οι πληροφορίες που παρέχονται από τους αισθητήρες διανέμονται στο σύστημα μέσα από μηχανισμούς του διαδικτύου για αυτό και τα WSN δεν πρέπει να θεωρούνται σαν ένα αυτόνομο δίκτυο μεταφοράς πληροφορίας. Με την χρήση του CoAP προσπαθούμε να εφαρμόσουμε τα βασικά στοιχεία του HTTP για μεταφορά δεδομένων της εφαρμογής χρησιμοποιώντας δίκτυα περιορισμένης δυνατότητας.[151]

Το CoAP χρησιμοποιεί το πρωτόκολλο UDP για τη διαχείριση των πόρων για να αποφευχθεί το overhead του TCP και να μειώσει τις απαιτήσεις του για bandwidth. Το CoAP υποστηρίζει τόσο unicast όσο και multicast σε αντίθεση με το TCP ικανοποιώντας την ανάγκη για ομαδική επικοινωνία. Επιπλέον το CoAP βασίζεται στην αρχιτεκτονική REST όπως και το HTTP που του παρέχει την δυνατότητα χρήσης των εντολών GET, POST, PUT, και DELETE, για δυνατότητα αλληλεπίδρασης σύμφωνα με τους πόρους σε μια αρχιτεκτονική πελάτη-διακομιστή, βοηθώντας έτσι να ξεπεραστεί η αναξιοπιστία του πρωτοκόλλου UDP. [153] Η χρήση του CoAP αποτελεί την πιο διαδεδομένη λύση σε εφαρμογές IoT και λαμβάνει σοβαρά

υπόψη την προστασία της επικοινωνίας μεταξύ των συσκευών, την προστασία από άποψη διαφάνειας (integrity), εχεμύθειας (confidentiality) και εξακρίβωσης ταυτότητας (authentication). [155] Το CoAP χρησιμοποιεί το DTLS πρωτόκολλο για προστασία των μεταδιδόμενων, αντίθετα όμως με άλλα πρωτόκολλα προστασίας που λειτουργούν στο επίπεδο δικτύου, το DTLS λειτουργεί στο επίπεδο εφαρμογής προσφέροντας προστασία στην end to end επικοινωνία μεταξύ το κόμβων. [151]

Για να επιτύχει στην προστασία των δεδομένων που ανταλλάσσονται μέσω του δικτύου χρησιμοποιεί 2-way authentication μέσω της χρήσης handshake. Το CoAP είναι δομημένο σε δύο στρώματα και αυτά απαρτίζονται από το κομμάτι των μηνυμάτων, που είναι υπεύθυνο να αλληλεπιδρά με το UDP (Message Layer), καθώς και το Request/Response κομμάτι που διαχειρίζεται την επικοινωνία πελάτη-εξυπηρετητή μέσω της εφαρμογής.

Abstract layer of CoAP [151]

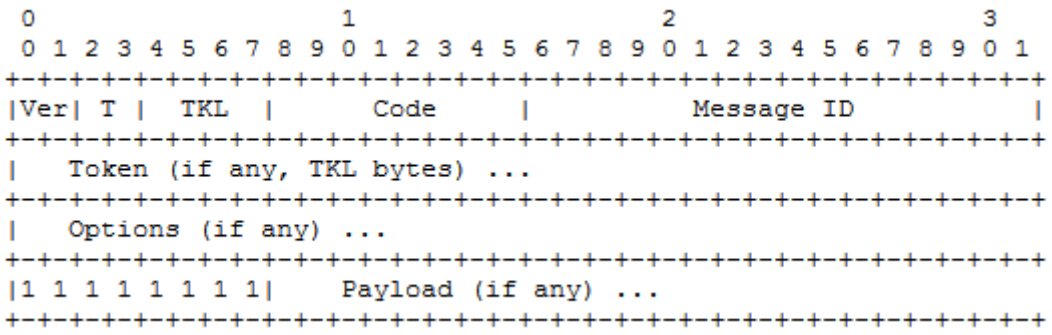
Το Message Layer του CoAP υποστηρίζει τέσσερις τύπους μηνυμάτων:

1. Μήνυμα αξιόπιστης μετάδοσης-CON (confirmable)
2. Μήνυμα αναξιόπιστης μετάδοσης-NON (non confirmable)
3. Μήνυμα επιβεβαίωσης λήψης-ACK (acknowledgement)
4. Μήνυμα επανάληψης αποστολής-RST (reset)

Οι ανταλλαγές μηνυμάτων μεταξύ αυτού του στρώματος και του UDP χαρακτηρίζονται από δυο κατηγορίες, την αξιόπιστη και την αναξιόπιστη μετάδοση μηνυμάτων. Η αξιοπιστία στην μετάδοση μηνυμάτων γίνεται χαρακτηρίζοντας το μήνυμα ως CON. [151],[153] Στην περίπτωση που για κάποιο μήνυμα δεν είναι απαραίτητη η χρήση αξιόπιστης μετάδοσης, υπάρχει η δυνατότητα ένα μήνυμα να σταλεί με τον χαρακτηρισμό NON. Ακόμα και μηνύματα που δεν χρειάζονται επιβεβαίωση, διαθέτουν ένα μοναδικό αναγνωριστικό (Message ID) έτσι ώστε να αποφευχθεί η αποστολή διπλότυπων μηνυμάτων. Όπως γίνεται στην περίπτωση της αξιόπιστης μετάδοσης, όταν ο παραλήπτης δεν μπορεί να επεξεργαστεί το μήνυμα που παρέλαβε έχει την δυνατότητα να στείλει ένα μήνυμα RST, αν και αυτό δεν είναι υποχρεωτικό. [153]

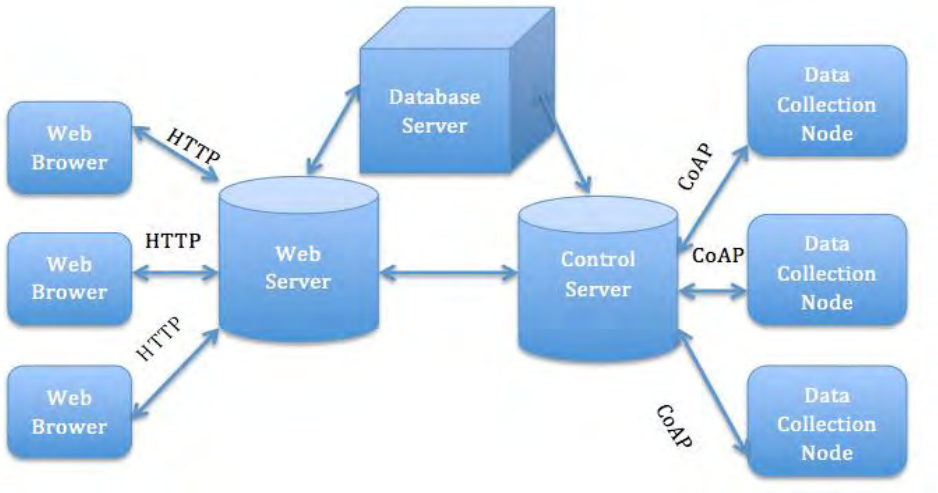
Το CoAP εξ' ορισμού βασίζεται στην ανταλλαγή μηνυμάτων μικρού μήκους, τα οποία μεταδίδονται μέσω UDP. Τα μηνύματα αυτά είναι σταθερού μεγέθους, χρησιμοποιούν δυαδική αναπαράσταση και αποτελούνται από την επικεφαλίδα (header) 4-byte, ένα token που εξαρτάται

από το μήκος της μεταβλητής και κυμαίνεται από 0-8 byte, τον αριθμό των επιλογών που συμπεριλαμβάνονται στο μήνυμα (Options), καθώς και το ωφέλιμο φορτίο (Payload). [154]



CoAP message format [154]

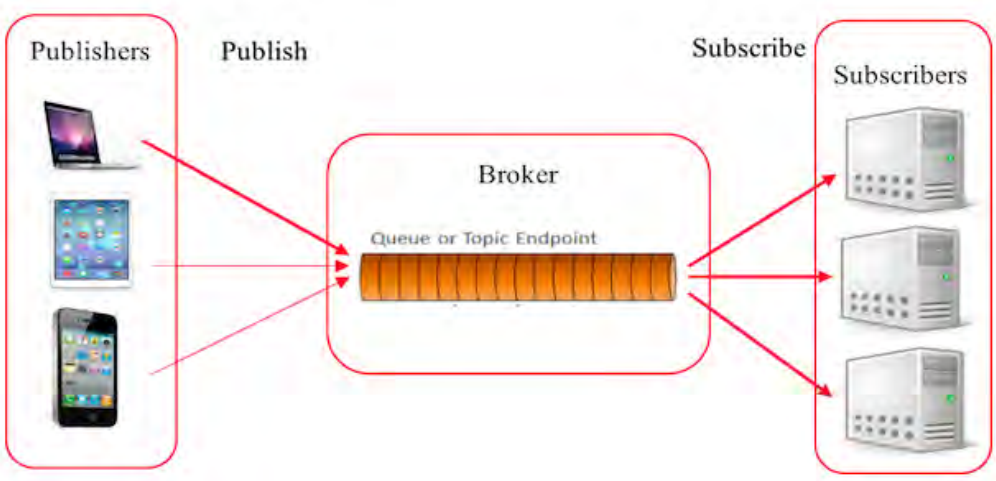
Το πρωτόκολλο CoAP λόγω των χαρακτηριστικών του μπορεί να θεωρηθεί ως η καλύτερη επιλογή πρωτοκόλλου σε οικιακά δίκτυα. Τα έξυπνα οικιακά δίκτυα παρέχουν έλεγχο και παρακολούθηση ενέργειας των οικιακών συσκευών. Τα συστήματα ελέγχου ενέργειας χρησιμοποιούν έξυπνη διαχείριση και παρακολούθηση της κατανάλωσης ενέργειας του εξοπλισμού για να παρέχουν πληροφορίες για την τάση, την τροφοδοσία και άλλες πληροφορίες σχετικά με την ενέργεια. Επιπλέον χαρακτηριστικά του είναι η προειδοποίηση σε περίπτωση ατυχήματος, ο απομακρυσμένος έλεγχος καθώς και η δυναμική εξοικονόμηση ενέργειας. Η δομή του συστήματος φαίνεται στην παρακάτω εικόνα. Κάθε κόμβος συλλογής δεδομένων μπορεί να ανταλλάξει πληροφορίες με άλλους κόμβους. Το CoAP θα μπορούσε να εγκατασταθεί τόσο σε τοπικά δίκτυα LAN αλλά και στο Διαδίκτυο. Σε αντίθεση με πολλά ασύρματα πρωτόκολλα για αυτόματες οικιακές συσκευές, το CoAP δεν είναι σχεδιασμένο για να περιορίζεται σε ένα τοπικό δίκτυο αλλά για να παρέχει τη θεμελιώδη βάση του Διαδικτύου.



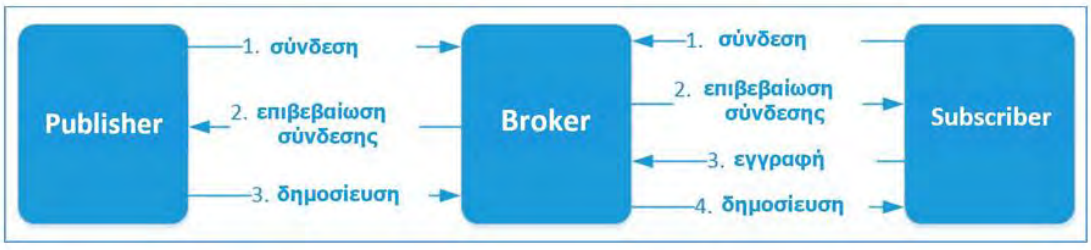
Σύστημα ελέγχου ενέργειας του πρωτοκόλλου CoAP [151]

Το πρωτόκολλο **Message Queue Telemetry Transport (MQTT)** αναπτύχθηκε από την IBM το 1999 και τυποποιήθηκε από την OASIS το 2018. Έχει σχεδιαστεί για να παρέχει ενσωματωμένη συνδεσιμότητα μεταξύ εφαρμογής και ενδιάμεσου λογισμικού από τη μια μεριά και δικτύου και επικοινωνιών από την άλλη μεριά.[155] Το πρωτόκολλο ακολουθεί την

publish/subscribe ασύγχρονη αρχιτεκτονική για την ανταλλαγή μηνυμάτων, που λειτουργεί στην κορυφή της TCP στοίβας στο επίπεδο εφαρμογής. Τα πρωτόκολλα τύπου publish/subscribe ανταποκρίνονται καλύτερα στις απαιτήσεις του IoT από τα πρωτόκολλα τύπου request/response αφού οι clients δεν χρειάζονται update κι έτσι το bandwidth μειώνεται και επεκτείνεται η διάρκεια ζωής των συσκευών που λειτουργούν με μπαταρία.[153] Το σύστημα αποτελείται από τρία κύρια δομικά στοιχεία: έναν κόμβο του δικτύου που ονομάζεται **publisher**, ο οποίος μπορεί να στέλνει μηνύματα σε έναν άλλον κόμβο (ή περισσότερους), που ονομάζεται **subscriber** με την χρήση ενός ενδιάμεσου διακομιστή που ονομάζεται **broker**. Η ανταλλαγή των μηνυμάτων πραγματοποιείται μεταξύ του client, που μπορεί να είναι publisher ή subscriber των μηνυμάτων και του broker των μηνυμάτων. Με την χρήστη του broker ως ενδιάμεσο κόμβο επιτυγχάνεται το φιλτράρισμα των μηνυμάτων και η παράδοση τους σε όλους τους ενδιαφερόμενους κόμβους.



Η αρχιτεκτονική του MQTT [155]



Σχέδιο απλής επικοινωνίας του subscriber, του publisher και του broker [156]

Το πρωτόκολλο MQTT σχεδιάστηκε για να χρησιμοποιεί bandwidth και μπαταρία με φειδώ και αυτό αποτελεί το λόγο για τον οποίο χρησιμοποιείται από το Facebook Messenger. Το MQTT εξασφαλίζει αξιοπιστία παρέχοντας την επιλογή ενός από τρία είδη QoS:

1. Fire and forget (QoS 0): ένα μήνυμα στέλνεται μια φορά χωρίς να επιβεβαιώνεται η λήψη τους

2. Delivered at least once (QoS 1): ένα μήνυμα στέλνεται τουλάχιστον μια φορά και αποθηκεύεται από τον αποστολέα έως ότου λάβει μήνυμα επιβεβαίωσης, διαφορετικά ξανά κάνει αποστολή του ίδιου μηνύματος
3. Delivered exactly once (QoS 2): είναι ο ασφαλέστερος μηχανισμός μετάδοσης αλλά ο πιο χρονοβόρος, όπου απαιτείται μηχανισμός σύναψης τετραπλής χειραψίας για να εξασφαλιστεί ότι το μήνυμα έχει παραδοθεί τουλάχιστον μια φορά [153]

Συνολικά, υπάρχουν 14 τύποι μηνυμάτων στο πρωτόκολλο MQTT οι οποίοι αναφέρονται αναλυτικά στο [156]. Επίσης, για να εξασφαλιστεί η ασφάλεια του MQTT, οι MQTT brokers μπορεί να χρειάζονται αυθεντικοποίηση με χρήση username/password την οποία χειρίζονται τα πρωτόκολλα TLS/SSL όπως συμβαίνει και με το HTTP.

Συγκρίνοντας τώρα το CoAP που αναφέραμε πριν με το MQTT, είναι πιθανό να παρατηρήσουμε ότι το CoAP που βασίζεται στο UDP έχει λιγότερο overhead σε σύγκριση με το MQTT που βασίζεται στο TCP. Εντούτοις, λόγω του μηχανισμού μη επαναποστολής μηνυμάτων του TCP, είναι πιο πιθανό να χαθούν πακέτα όταν χρησιμοποιούμε το CoAP. Σύμφωνα με τη μελέτη [157], το MQTT υφίσταται μικρότερες καθυστερήσεις από το CoAP για μικρές απώλειες πακέτων, αλλά το CoAP δημιουργεί λιγότερη έξτρα κίνηση για την εξασφάλιση αξιοπιστίας. Παρόλα αυτά, τα αποτελέσματα μπορεί να ποικίλουν ανάλογα με τις συνθήκες του κάθε δικτύου. Επιπλέον, οι απώλειες πακέτων και οι καθυστερήσεις εξαρτώνται και από το QoS των μηνυμάτων. Τέλος, και στα δύο πρωτόκολλα, η απώλεια πακέτων μειώνεται και οι καθυστερήσεις αυξάνονται όταν το επίπεδο του QoS είναι υψηλό. [153]

2.2.6 Παραδείγματα IoT Εφαρμογών [161]

Το IoT είναι κάτι περισσότερο από μια ευκολία για τους καταναλωτές. Προσφέρει νέες πηγές δεδομένων και νέα επιχειρηματικά μοντέλα που μπορούν να ενισχύσουν την παραγωγικότητα σε διάφορους κλάδους. Το IoT διεισδύει σε αμέτρητες εφαρμογές, οι οποίες περιλαμβάνουν σχεδόν όλο το σύνολο των αγορών και των σημερινών υπηρεσιών.

Έξυπνες λύσεις μεταφοράς επιταχύνουν την ροή της κυκλοφορίας, μειώνουν την κατανάλωση καυσίμων, προτεραιοποιούν τα προγράμματα επισκευής οχημάτων και σώζουν ζωές.

Έξυπνα ηλεκτρικά δίκτυα (smart electric grids) συνδέουν πιο αποτελεσματικά ανανεώσιμες πηγές ενέργειας, βελτιώνουν την αξιοπιστία του συστήματος και χρεώνουν τους καταναλωτές με βάση μικρότερες προσαυξήσεις.

Μηχανές αισθητήρων παρακολούθησης κάνουν διαγνώσεις και προβλέπουν θέματα συντήρησης που εκκρεμούν, βραχυπρόθεσμα stock-out αποθεμάτων, και θέτουν ακόμα και προτεραιότητες στα προγράμματα του προσωπικού που είναι υπεύθυνο για τις επισκευές για να καλύψουν αποτελεσματικότερα τις ανάγκες επισκευής εξοπλισμού αλλά και περιφερειακές ανάγκες.

Data-driven συστήματα, χτισμένα στις υποδομές των έξυπνων πόλεων βοηθούν τους ανθρώπους να απαλλαχτούν από μερικά από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν σήμερα. Μερικά παραδείγματα εφαρμογών για έξυπνες πόλεις είναι το έξυπνο Parking, η πολεοδομική «υγεία», οι χάρτες αστικού θορύβου, η ανίχνευση μέσω smartphones, η κυκλοφοριακή αποσυμφόρηση, ο έξυπνος φωτισμός, οι έξυπνοι δρόμοι και το σύστημα διαχείρισης αποβλήτων.

Το IoT προσθέτει περισσότερη αξία στην βιομηχανία της υγειονομικής περίθαλψης. Λόγω του IoT, μερικά πλεονεκτήματα τα οποία θα προστεθούν στον τομέα της φροντίδας υγείας είναι: η ανίχνευση πτώσης, τα ιατρικά ψυγεία, η φροντίδα υγείας αθλητών, η επιτήρηση των ασθενών, η μέτρηση της υπεριώδους ακτινοβολίας κ.α.

Ενώ τα αυτοκίνητα δεν έχουν φτάσει ακόμα στο σημείο να μετακινούνται αυτόνομα, είναι αναμφισβήτητα πιο τεχνολογικά προηγμένα από ποτέ. Τα συνδεδεμένα οχήματα θα μπορούσαν να μειώσουν δραματικά τον αριθμό των θανάτων και των σοβαρών τραυματισμών που προκλήθηκαν από ατυχήματα στους δρόμους και στους αυτοκινητόδρομους. Η τεχνολογία των συνδεδεμένων οχημάτων θα επιτρέψει σε αυτοκίνητα, φορτηγά, λεωφορεία και άλλα οχήματα να "μιλούν" μεταξύ τους με ενσωματωμένες στο αυτοκίνητο συσκευές που μοιράζονται συνεχώς σημαντικές πληροφορίες για την ασφάλεια και την κινητικότητα.

Στον τομέα της διαχείρισης πόρων του περιβάλλοντος και των οικολογικών δράσεων, οι εφαρμογές του IoT θα μπορούσαν να περιλαμβάνουν την παρακολούθηση πληθυσμών απειλούμενων ζώων, την επίβλεψη δασικών οικοσυστημάτων για την πρόβλεψη πυρκαγιών, την πρόβλεψη έντονων καιρικών φαινομένων, την πρόληψη κατά της ρύπανσης του υδροφόρου ορίζοντα και την καλύτερη αξιοποίηση των αποθεμάτων νερού.

Ένα έξυπνο σπίτι είναι ένα πλήρως αυτοματοποιημένο σπίτι που βοηθά τους κατοίκους του να ζουν με άνεση και ασφάλεια. Ένα δίκτυο έξυπνων εξαρτημάτων (ενσύρματων ή και ασύρματων) βρίσκεται παντού μέσα σε κάθε χώρο του σπιτιού, σε κάθε διακόπτη, σε κάθε ηλεκτρικό πίνακα. Το δίκτυο αυτό συμπληρώνει ένα δίκτυο αισθητήρων που παρέχουν χρήσιμες πληροφορίες. Όλα τα εξαρτήματα και οι αισθητήρες ανταλλάσσουν μεταξύ τους πληροφορίες και εκτελούν ενέργειες βάση του προκαθορισμένου προγραμματισμού που έχουν λάβει.

Όπως είδαμε, υπάρχει ένα εύρος εφαρμογών σε διαφορετικούς τομείς, που μπορούν να αναπτυχτούν στα πλαίσια του IoT. Για την ανάπτυξη τους όμως και την τελική τους χρήση σε ευρεία κλίμακα, είναι αναγκαία η συμμετοχή και η συνεργασία αρκετών επιμέρους οργανισμών. Η ανάγκη αυτή αποτελεί ταυτόχρονα και επιχειρηματική ευκαιρία για τους οργανισμούς αυτούς που θα κληθούν να επενδύσουν και να αξιοποιήσουν τις επενδύσεις τους. Γίνεται λοιπόν εμφανές, πως τόσο κατά τη μετάβαση στο IoT, όσο και μετά, θα δημιουργηθούν οι κατάλληλες συνθήκες για την ανάπτυξη και την πρόοδο της επιστήμης της τεχνολογίας.

Κεφάλαιο 3: Πρωτόκολλα για WSN/IoT

3.1 Αλγόριθμοι δρομολόγησης σε δίκτυα WSN/IoT

Στο Επίπεδο Δικτύου (Network Layer), της Στοίβας Πρωτοκόλλων των WSN, ανήκουν οι αλγόριθμοι ή πρωτόκολλα δρομολόγησης, χάρη στα οποία είναι εφικτή η επιτυχής παράδοση των πακέτων δεδομένων στον κόμβο-συλλέκτη (sink). Οι ιδιαιτερότητες των WSN δεν επιτρέπουν τη χρήση παραδοσιακών αλγορίθμων, αφού ένας αλγόριθμος δρομολόγησης σε ασύρματα δίκτυα αισθητήρων οφείλει να λαμβάνει υπόψη του στοιχεία όπως η τυχαία-αδόμητη μορφή, η περιορισμένη ενεργειακή αυτονομία, οι μειωμένες υπολογιστικές ικανότητες, η ανοχή σε σφάλματα λειτουργίας, η μικρή εμβέλεια εκπομπής - οποία οδηγεί σε μετάδοση πολλαπλών αναπηδήσεων (multiple hops transmission) - ο υψηλός αριθμός και η αυξημένη πυκνότητα των κόμβων, το μέσο διάδοσης και τα ενδεχόμενα συγκρούσεων (collisions). Επίσης, μιας και η

ανάπτυξη πρωτοκόλλων στα WSN πρέπει να είναι προσαρμοσμένη στην εκάστοτε εφαρμογή (application specific), χρειάζεται πολλές φορές να ικανοποιούνται ζητήματα ποιότητας υπηρεσίας (Quality of Service – QoS), όπως ο μικρός χρόνος καθυστέρησης στην παράδοση του πακέτου.

Η παρακάτω ταξινόμηση των αλγορίθμων για ασύρματα δίκτυα αισθητήρων είναι ενδεικτική και σίγουρα δεν μπορεί να περιγράψει πλήρως την ποικιλία των διαδικασιών δρομολόγησης που προκύπτει ως απόρροια της ποικιλομορφίας των εφαρμογών των WSN. Συνηθέστερα, τα πρωτόκολλα δρομολόγησης έχουν περισσότερο υβριδικό χαρακτήρα, αφού σχεδιάζονται με στοιχεία που εμπίπτουν ταυτόχρονα σε περισσότερες από μια από τις κατηγορίες που θα αναφερθούν:

Αλγόριθμοι με Επίκεντρο τα Δεδομένα (Data-centric Algorithms):

Δεδομένου του υψηλού, συνήθως, αριθμού κόμβων-αισθητήρων σε ένα WSN δεν είναι εφικτή η εκχώρηση καθολικών ταυτοτήτων (global identifiers) σε όλους τους κόμβους. Επιπλέον, λόγω της υψηλής πυκνότητας, υπάρχει πλεόνασμα πληροφορίας, αφού δύο οι περισσότεροι κόμβοι μπορεί να ελέγχουν την ίδια περιοχή. Αυτό οδήγησε στην ανάπτυξη τεχνικών δρομολόγησης με προσανατολισμό στα δεδομένα οι οποίες διαφοροποιούνται από την κλασσική address-based δρομολόγηση. Στην data-centric δρομολόγηση ο κόμβος-συλλέκτης αποστέλλει αιτήματα σε συγκεκριμένες περιοχές του υπό επιτήρηση χώρου και αναμένει τα δεδομένα ανίχνευσης των κόμβων που βρίσκονται στις περιοχές αυτές. Παραδείγματα αλγορίθμων αυτού του τύπου είναι οι: SPIN [191], Directed Diffusion [192], Rumor Routing [193], GBR [194], CADR [195].

Ιεραρχικοί Αλγόριθμοι (Hierarchical Algorithms):

Ο μεγάλος αριθμός κόμβων μπορεί να οδηγήσει σε υπερφόρτωση του δικτύου, προκαλώντας σημαντική καθυστέρηση στην επικοινωνία και ανεπαρκή παρακολούθηση των μεταβολών των υπό μέτρηση μεταβλητών. Για την κάλυψη, λοιπόν, μεγάλων περιοχών χωρίς υποβιβασμό των παρεχομένων από το δίκτυο υπηρεσιών, προτείνεται από τους Ιεραρχικούς αλγορίθμους η διαδικασία του clustering. Με αυτό τον τρόπο επιτυγχάνεται χαμηλότερη κατανάλωση ενέργειας και μικρότερος αριθμός εκπεμπόμενων μηνυμάτων προς τον κόμβο-συλλέκτη. Παραδείγματα αυτού του τύπου: LEACH [196], PEGASIS [197], TEEN [198], APTEEN [199]

Γεωγραφικοί Αλγόριθμοι (Geographic Algorithms):

Δεδομένου ότι δεν υπάρχει σύστημα διευθυνσιοδότησης στα WSN, όπως οι διευθύνσεις IP, και οι κόμβοι είναι χωρικά τοποθετημένοι με τυχαίο τρόπο, η πληροφορία των θέσεων των κόμβων αισθητήρων μπορεί να χρησιμοποιηθεί για δρομολόγηση με ενεργειακά αποδοτικό τρόπο. Στη συγκεκριμένη κατηγορία εντάσσονται και κάποιοι αλγόριθμοι δρομολόγησης σε Κινητά Αδόμητα Δίκτυα (Mobile Ad-Hoc Networks – MANETS), οι οποίοι ικανοποιούν το κριτήριο της Ενεργειακής αποδοτικότητας. Παραδείγματα αυτής της κατηγορίας: MECN [200], GAF [201], GEAR [202] ,GeRaF [203][204].

Αλγόριθμοι Δικτυακής Ροής και Ποιότητας Υπηρεσιών (Network flow & QoS Algorithms):

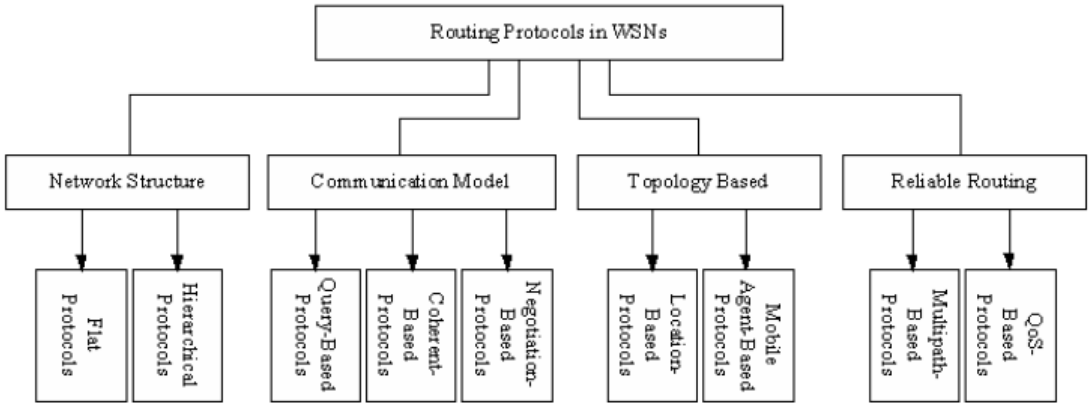
Πρόκειται για ειδική κατηγορία αλγορίθμων στην οποία η διαδικασία της δρομολόγησης είτε μοντελοποιείται και επιλύεται ως πρόβλημα δικτυακής ροής είτε λαμβάνει υπόψη παράγοντες ποιότητας υπηρεσιών, κυρίως όσον αφορά την έγκαιρη παράδοση των πακέτων. Παραδείγματα της κατηγορίας: Maximum lifetime energy routing [205], Maximum lifetime data gathering [206], Minimum cost forwarding [207], SAR [208], SPEED [209].

3.2 Επισκόπηση ενεργειακά αποδοτικών πρωτοκόλλων

Η εξοικονόμηση της ενέργειας στα ασύρματα δίκτυα αισθητήρων είναι μια αποφασιστική πρόκληση στον σχεδιασμό πρωτοκόλλων. Είναι, λοιπόν, απαραίτητη η επινόηση τηλεπικοινωνιακών και δικτυακών σχημάτων τα οποία θα κάνουν συνετή χρήση των περιορισμένων ενεργειακών αποθεμάτων των κόμβων-αισθητήρων χωρίς συμβιβασμούς στη συνδεσιμότητα του δικτύου.

Ένας συνηθισμένος μηχανισμός εξοικονόμησης ενέργειας είναι η χρήση κύκλου λειτουργίας στο επίπεδο Ελέγχου Πρόσβασης Μέσου (MAC Layer), βάσει του οποίου οι κόμβοι εισέρχονται σε καταστάσεις αδράνειας (sleep mode) με συχνότητα και διάρκεια που δεν ακυρώνει τη συνδεσιμότητα του δικτύου. Παραδείγματα τέτοιων αλγορίθμων που βασίζονται σε αυτή την τεχνική, είναι οι SPAN [210], GAF [211], STEM [212]. Κοινό χαρακτηριστικό των παραπάνω πρωτοκόλλων είναι η γνώση της τοπολογίας του δικτύου, έστω και μερική σε κάποιες περιπτώσεις, αφού ο κάθε κόμβος πρέπει να γνωρίζει τους γείτονές του, δηλαδή τους κόμβους εντός της εμβέλειάς του, και πιθανώς κάποια επιπλέον πληροφορία όσον αφορά τις διαθέσιμες διαδρομές προς τον επιθυμητό προορισμό.

Παρακάτω ακολουθεί κατηγοριοποίηση των πρωτοκόλλων δρομολόγησης για τα ασύρματα δίκτυα αισθητήρων όπως φαίνεται και στο σχήμα:



Κατηγοριοποίηση πρωτοκόλλων στα Ασύρματα Δίκτυα αισθητήρων. [188]

1) Πρωτόκολλα Βασισμένα στη δομή του δικτύου (Network Structure)

Η δομή του δικτύου συχνά καθορίζεται από την ομοιομορφία των κόμβων. Το κύριο είναι ο τρόπος που οι κόμβοι συνδέονται και δρομολογούν τις πληροφορίες βασιζόμενοι στην υποκείμενη αρχιτεκτονική. Αυτό δημιουργεί δύο τύπους τοποθέτησης κόμβων, στο **ίδιο επίπεδο σύνδεσης** και **σε ιεραρχίες**. Ως εκ τούτου, τα πρωτόκολλα αυτής της κατηγορίας μπορούν να ταξινομηθούν περαιτέρω ως εξής:

- ***Επίπεδα Πρωτόκολλα* (*Flat Protocols)*** όπου όλοι οι κόμβοι του δικτύου παίζουν τον ίδιο ρόλο.
- ***Ιεραρχικά Πρωτόκολλα (Hierarchical Protocols)*** στα οποία οι κόμβοι του δικτύου οργανώνονται σε συμπλέγματα-συστάδες όπου ο κόμβος με την υψηλότερη στάθμη ενέργειας, για παράδειγμα, αναλαμβάνει το ρόλο του επικεφαλής του συμπλέγματος. Η ομαδοποίηση των κόμβων έχει τη δυνατότητα να μειώσει την κατανάλωση ενέργειας και

να παρατείνει τη διάρκεια ζωής του δικτύου. Έχει υψηλή αναλογία παράδοσης δεδομένων και επεκτασιμότητας και μπορεί να ισορροπήσει την κατανάλωση ενέργειας. Οι κόμβοι γύρω από το σταθμό βάσης ή τον επικεφαλής καταναλώνουν πιο γρήγορα την διαθέσιμη ενέργεια τους από τους άλλους κόμβους.

2) Πρωτόκολλα Βασισμένα στο Μοντέλο Επικοινωνίας (Communication Model)

Το μοντέλο επικοινωνίας σε ένα πρωτόκολλο δρομολόγησης σχετίζεται με τον τρόπο που ακολουθείται η κύρια λειτουργία του πρωτοκόλλου για τη δρομολόγηση πακέτων στο δίκτυο. Τα πρωτόκολλα αυτής της κατηγορίας μπορεί να παραδώσουν περισσότερα δεδομένα για μια δεδομένη ποσότητα ενέργειας. Επίσης, όσον αφορά το
ποσοστό διάδοσης και χρήσης της ενέργειας τα πρωτόκολλα αυτής της κατηγορίας μπορούν να εκτελέσουν πολύ κοντά στο θεωρητικό βέλτιστο από σημείο-σε-σημείο και σε δίκτυα ανοικτής εκπομπής. Επίσης διακρίνονται σε:

- ***Πρωτόκολλα βασισμένα στο Ερώτημα (Query-Based)****:* Οι κόμβοι προορισμού διαδίδουν ένα αίτημα για δεδομένα από έναν κόμβο μέσω του δικτύου και ο κόμβος που έχει τα δεδομένα στέλνει, αυτά που ταιριάζουν με το ερώτημα, πίσω στον κόμβο.
- ***Συνεκτικά και μη-Συνεκτικά Πρωτόκολλα (Coherent and Non-Coherent- Based)****:* όπου τα δεδομένα προωθούνται σε συναθροιστές μετά από μια ελάχιστη επεξεργασία ή οι κόμβοι επεξεργάζονται τοπικά τα ανεπεξέργαστα δεδομένα πριν αποσταλούν σε άλλους κόμβους για περαιτέρω επεξεργασία.
- ***Πρωτόκολλα βασισμένα στην Διαπραγμάτευση (Negotiation-Based)****:* Χρησιμοποιούν τις διαπραγματεύσεις των μετά-δεδομένων για να μειωθούν οι περιττές μεταδόσεις στο δίκτυο.

3) Πρωτόκολλα βασισμένα στην Τοπολογία (Topology Based)

Τα πρωτόκολλα αυτά χρησιμοποιούν την αρχή ότι κάθε κόμβος σε ένα δίκτυο διατηρεί πληροφορίες τοπολογίας και ότι η κύρια διαδικασία της λειτουργίας του πρωτοκόλλου βασίζεται στην τοπολογία του δικτύου. Τα πρωτόκολλα αυτά μπορούν
να ταξινομηθούν περαιτέρω ως εξής:

- ***Πρωτόκολλα βασισμένα στην Θέση (Location-based):*** Τα πρωτόκολλα αυτά μπορεί να επωφεληθούν από τις πληροφορίες θέσης, προκειμένου να αναμεταδώσουν τα δεδομένα που έλαβαν μόνο σε ορισμένες περιοχές και όχι σε ολόκληρο το WSN, γεγονός που οδηγεί σε ελαχιστοποίηση της κατανάλωσης ενέργειας των κόμβων αισθητήρων.
- ***Πρωτόκολλα βασισμένα σε Κινητούς Πράκτορες (Mobile Agent-based):*** Τα συστήματα κινητών πρακτόρων έχουν ως κύριο συστατικό ένα κινητό μέσο, το οποίο μετακινείται μεταξύ των κόμβων ενός δικτύου για να εκτελέσει μια εργασία αυτόνομα και έξυπνα, με βάση τις συνθήκες του περιβάλλοντος.

4) Πρωτόκολλα βασισμένα στην Αξιόπιστη Δρομολόγηση (Reliable Routing)

Τα πρωτόκολλα αυτά είναι πιο ανθεκτικά σε προβληματικές διαδρομές είτε με την εύρεση εναλλακτικών διαδρομών ή πληρώντας ορισμένες παραμέτρους QoS, όπως η καθυστέρηση, η ενέργεια, και το εύρος ζώνης. Τα πρωτόκολλα αυτά ταξινομούνται ως εξής:

- ***Πρωτόκολλα βασισμένα σε πολλαπλές διαδρομές (Multipath-Based):***

Επιτυγχάνουν την εξισορρόπηση του φορτίου και είναι πιο ανθεκτικά σε προβληματικές διαδρομές.

- ***Πρωτόκολλα βασισμένα στην ποιότητα υπηρεσίας (QoS-based):*** Το δίκτυο θα πρέπει να ισορροπήσει μεταξύ της κατανάλωσης ενέργειας και της ποιότητας της υπηρεσίας. [187,188]

Παρακάτω γίνεται αναφορά των πιο γνωστών ενεργειακά αποδοτικών πρωτοκόλλων δρομολόγησης.

SPIN

Το SPIN ανήκει στα Επίπεδα Πρωτόκολλα δρομολόγησης (Flat Protocols). Τα πρωτόκολλα δρομολόγησης τα οποία είναι βασισμένα στην διαπραγμάτευση SPIN (Sensor Protocols for Information via Negotiation) αποτελούν μια ομάδα πρώιμων έργων για κεντρικοποιημένη (data-centric) δρομολόγηση. Η οικογένεια των πρωτοκόλλων SPIN βασίζεται σε δύο βασικές ιδέες.

- Πρώτον, για να λειτουργεί αποτελεσματικά και να εξοικονομεί ενέργεια το πρωτόκολλο, οι κόμβοι πρέπει να επικοινωνούν μεταξύ τους σχετικά με τα δεδομένα που έχουν ήδη και τα δεδομένα που πρέπει να λάβουν.
- Δεύτερον, οι κόμβοι σε ένα δίκτυο πρέπει να παρακολουθούν και να προσαρμόζονται σε αλλαγές στους ενεργειακούς πόρους τους ώστε να παρατείνουν τη διάρκεια λειτουργίας του συστήματος.

Η κύρια ιδέα του SPIN είναι ο χαρακτηρισμός των δεδομένων χρησιμοποιώντας περιγραφείς υψηλού επιπέδου ή μετά-δεδομένα. Χρησιμοποιούν μετά-δεδομένα για τη μείωση των περιττών μεταδόσεων στο δίκτυο. Ως εκ τούτου, αν ένας κόμβος έχει κάποια δεδομένα, πρώτα απ' όλα, τα διαφημίζει με την αποστολή ενός πακέτου διαφήμισης (ADV) στους άλλους κόμβους και αν κάποιος κόμβος που λάβει το διαφημιζόμενο πακέτο ενδιαφέρεται για τα δεδομένα τότε στέλνει ένα πακέτο αιτήματος (REQ) και κατά τη λήψη του πακέτου αίτησης ο κόμβος στέλνει τα πραγματικά δεδομένα (DATA). Το πρόβλημα με το SPIN είναι ότι δεν εγγυάται την παράδοση των δεδομένων. [191]

Direct Diffusion (DD)

Το πρωτόκολλο Κατευθυνόμενης διάχυσης (DD) ανήκει στα Επίπεδα Πρωτόκολλα δρομολόγησης (Flat Protocols). Το DD μπορεί να επιλέξει εμπειρικά καλές διαδρομές και να χρησιμοποιήσει τις τεχνικές της γρήγορης μνήμης και της επεξεργασίας δεδομένων στο δίκτυο, προκειμένου να επιτύχει την ελαχιστοποίηση της κατανάλωσης ενέργειας.

Το DD έχει τη δυνατότητα για σημαντική μείωση της ενεργειακής κατανάλωσης των κόμβων και για παράταση της διάρκειας ζωής του δικτύου. Ακόμη και με την επιλογή μιας σχετικά μη βέλτιστης διαδρομής, υπερτερεί από ένα ιδεατό παραδοσιακό σύστημα διάδοσης δεδομένων όπως η πολυεκπομπή. Επιπλέον, το DD είναι σταθερό. [192]

Rumor Routing (RR)

Το πρωτόκολλο Φήμης ανήκει στα Επίπεδα Πρωτόκολλα δρομολόγησης (Flat Protocols). Η δρομολόγηση φήμης είναι ένας συμβιβασμός μεταξύ των πλημμύρων και των ειδοποιήσεων. Η κύρια ιδέα αυτού του πρωτοκόλλου είναι ότι δημιουργεί μονοπάτια που οδηγούν σε κάθε συμβάν, σε αντίθεση με τις πλημμύρες που δημιουργούν ένα πεδίο διαδρομών σε ολόκληρο το δίκτυο. Έτσι, σε περίπτωση που δημιουργείται ένα αίτημα, μπορεί το αίτημα αυτό να αποσταλεί σε ένα τυχαίο μονοπάτι μέχρι να βρει το συμβάν, αντί των πλημμύρων που στέλνονται σε όλο το δίκτυο. Η δρομολόγηση φήμης μπορεί να είναι μια καλή μέθοδος για την παράδοση αιτημάτων σε μεγάλα δίκτυα, σύμφωνα με ένα ευρύ φάσμα συνθηκών (χαμηλότερες ενεργειακές απαιτήσεις από εναλλακτικές λύσεις). Είναι σχεδιασμένη να είναι προσαρμόσιμη σε διαφορετικές εφαρμογές και υποστηρίζει διάφορα αιτήματα σε ανάλογες εκδηλώσεις, με υψηλά ποσοστά επιτυχούς παράδοσης και επισκευής διαδρομής. Επιπλέον, είναι σε θέση να χειριστεί την αποτυχία κόμβων, υποβαθμίζοντας το ρυθμό παράδοσης γραμμικά με τον αριθμό των αποτυχημένων κόμβων. [193]

LEACH (Low-energy adaptive clustering hierarchy)

Το πρωτόκολλο Χαμηλής Ενέργειας Προσαρμοσμένων Συστάδων είναι ένα ιεραρχικό πρωτόκολλο στο οποίο οι περισσότεροι κόμβοι μεταδίδουν τα δεδομένα στους επικεφαλής κόμβους. Η λειτουργία του πρωτοκόλλου LEACH αποτελείται από δύο φάσεις:

- *Φάση εγκατάστασης.* Στην φάση εγκατάστασης, πρώτα οργανώνονται οι συστάδες και επιλέγονται οι επικεφαλής. Οι επικεφαλής συγκεντρώνουν, συμπιέζουν και διαβιβάζουν τα δεδομένα στο σταθμό βάσης. Κάθε κόμβος καθορίζει αν θα γίνει επικεφαλής, σε αυτό το γύρο, με τη χρήση ενός αλγορίθμου. Αυτή η περιστροφή στην επιλογή επικεφαλής οδηγεί σε ισορροπημένη κατανάλωση ενέργειας σε όλους τους κόμβους και συνεπώς σε μεγαλύτερη διάρκεια ζωής του δικτύου.
- *Σταθερή φάση.* Στη σταθερή φάση, τα δεδομένα αποστέλλονται στο σταθμό βάσης. Η διάρκεια της σταθερής φάσης είναι μεγαλύτερη σε διάρκεια από την φάση εγκατάστασης, προκειμένου να ελαχιστοποιηθεί η πολυπλοκότητα. Επιπλέον, κάθε κόμβος που δεν είναι επικεφαλής επιλέγει τον πλησιέστερο επικεφαλής για να στείλει τα δεδομένα του.

Το κύριο πλεονέκτημα του LEACH είναι ότι ξεπερνά τα συμβατικά πρωτόκολλα επικοινωνίας, από την άποψη της εξοικονόμησης ενέργειας, της ευκολίας της διαμόρφωσης, και της διάρκειας ζωής του συστήματος/ ποιότητας του δικτύου. Ωστόσο, το LEACH χρησιμοποιεί δρομολόγηση ενός βήματος όπου κάθε κόμβος μπορεί να μεταδώσει απευθείας στον επικεφαλής και στον σταθμό βάσης. Ως εκ τούτου, δεν συνιστάται για δίκτυα που καλύπτουν μεγάλες περιοχές. Επιπλέον, η δυναμική ομαδοποίηση οδηγεί σε επιπλέον επιβάρυνση, π.χ. για την αλλαγή του επικεφαλής, τις διαφημίσεις κλπ., η οποία μπορεί να μειώσει το κέρδος στην κατανάλωση ενέργειας. [196]

LEACH-C (LEACH-Centralized)

Το πρωτόκολλο Χαμηλής Ενέργειας Κεντρικοποιημένων Συστάδων είναι ένα ιεραρχικό πρωτόκολλο το οποίο χρησιμοποιεί το σταθμό βάσης (BS) για το σχηματισμό συστάδων, σε αντίθεση με το LEACH όπου οι κόμβοι οι ίδιοι οργανώνονται σε συστάδες. Οι βελτιώσεις αυτού του αλγορίθμου σε σύγκριση με το LEACH είναι οι ακόλουθες:

- Ο BS χρησιμοποιεί την γνώση του δικτύου για την οργάνωση των συστάδων που απαιτούν τη λιγότερη ενέργεια για τη μετάδοση των δεδομένων.
- Σε αντίθεση με το LEACH, όπου ο αριθμός των επικεφαλής ποικίλλει από γύρο σε γύρο λόγω της έλλειψης συντονισμού μεταξύ των κόμβων, στο LEACH-C ο αριθμός των επικεφαλής συστάδας σε κάθε γύρο ισούται με μία προκαθορισμένη βέλτιστη τιμή. [196]

PEGASIS (Power efficient gathering in sensor information systems)

Το πρωτόκολλο Ενεργειακής Απόδοσης Συλλογής είναι ένα ιεραρχικό πρωτόκολλο που βασίζεται στην αλυσίδα και αποτελεί βελτίωση του LEACH. Στο PEGASIS κάθε κόμβος επικοινωνεί μόνο με ένα κοντινό γείτονα, προκειμένου να στείλει και να λάβει δεδομένα. Σε κάθε γύρο μεταδίδει τα δεδομένα στο σταθμό βάσης, μειώνοντας έτσι την ποσότητα της ενέργειας που δαπανάται σε κάθε γύρο. Οι κόμβοι οργανώνονται κατά τέτοιο τρόπο ώστε να σχηματίσουν μια αλυσίδα, η οποία μπορεί να επιτευχθεί είτε από τους ίδιους τους κόμβους αισθητήρων, χρησιμοποιώντας ένα άπληστο αλγόριθμο ξεκινώντας από κάποιο κόμβο, ή μπορεί ο BS να υπολογίσει αυτή την αλυσίδα και να ενημερώσει τους κόμβους.

Σε γενικές γραμμές, το πρωτόκολλο PEGASIS παρουσιάζει περισσότερες φορές καλύτερη απόδοση σε σύγκριση με το πρωτόκολλο LEACH. Ωστόσο, το πρωτόκολλο PEGASIS προκαλεί την μετάδοση περιττών δεδομένων από τους κόμβους στην αλυσίδα. Η αιτία αυτού του προβλήματος είναι ότι δεν υπολογίζεται η τοποθεσία του σταθμού βάσης για την ενέργεια των κόμβων, όταν ένας από τους κόμβους επιλέγεται ως επικεφαλής. [197]

TEEN (Threshold sensitive energy-efficient sensor network)

Το πρωτόκολλο Ευαίσθητου Ορίου Δικτύου Αισθητήρων είναι ένα ιεραρχικό πρωτόκολλο σχεδιασμένο για συνθήκες, οι οποίες περιλαμβάνουν αιφνίδιες αλλαγές σε χαρακτηριστικά όπως η θερμοκρασία. Η αρχιτεκτονική του δικτύου αισθητήρων στο TEEN βασίζεται σε μια ιεραρχική ομαδοποίηση των κόμβων. Σε αυτό το πρωτόκολλο ο επικεφαλής εκπέμπει προς τα μέλη του ένα άνω αυστηρό όριο (Hard Threshold) και ένα κάτω ήπιο όριο (Soft Threshold). Οι κόμβοι ανιχνεύουν το περιβάλλον τους συνεχώς. Την πρώτη φορά που μια παράμετρος από τα μετρήσιμα χαρακτηριστικά φτάνει σε Hard Threshold, ο κόμβος στέλνει τα δεδομένα που ανιχνεύονται. Η ανιχνευμένη τιμή αποθηκεύεται σε μία εσωτερική μεταβλητή στον κόμβο, που ονομάζεται ανιχνευμένη τιμή (Sensed Value). Το κύριο πλεονέκτημα του TEEN είναι ότι λειτουργεί καλά σε συνθήκες με αιφνίδιες αλλαγές στις τιμές του περιβάλλοντος, όπως η θερμοκρασία. Από την άλλη πλευρά, σε μεγάλα δίκτυα και όταν ο αριθμός των επιπέδων στην ιεραρχία είναι μικρός, το TEEN τείνει να καταναλώνει πολύ ενέργεια, λόγω της μεγάλης απόστασης μεταξύ των μεταδόσεων. Επιπλέον, όταν ο αριθμός των επιπέδων αυξάνεται, οι μεταδόσεις γίνονται μικρότερες. [198]

APTEEN (Adaptive threshold sensitive energy efficient sensor network)

Το πρωτόκολλο Προσαρμοσμένου Ευαίσθητου Ορίου Δικτύου Αισθητήρων αποτελεί βελτίωση του TEEN και στοχεύει τόσο στην καταγραφή της περιοδικής συλλογής δεδομένων όσο και στο να αντιδρά σε χρονικά κρίσιμα γεγονότα. Μόλις ο σταθμός βάσης σχηματίσει τις συστάδες, οι

επικεφαλής μεταδίδουν τα χαρακτηριστικά, τις τιμές κατωφλίου και το χρονοδιάγραμμα μετάδοσης σε όλους τους κόμβους. Μετά από αυτό οι επικεφαλής εκτελούν την συνάθροιση δεδομένων, η οποία έχει ως αποτέλεσμα την εξοικονόμηση ενέργειας. Το κύριο πλεονέκτημα του APTEEN, σε σύγκριση με το TEEN είναι ότι οι κόμβοι καταναλώνουν λιγότερη ενέργεια. Ωστόσο, τα κύρια μειονεκτήματα του APTEEN είναι η πολυπλοκότητά του και το ότι οδηγεί σε μεγάλες χρονικές καθυστέρησης. [199]

ECHERP

Το ECHERP είναι ένα ενεργειακά αποδοτικό πρωτόκολλο που σε αντίθεση με τα άλλα υπάρχον πρωτόκολλα που επιλέγουν ένα τυχαίο κόμβο ή τον κόμβο με την υψηλότερη ενέργεια μια συγκεκριμένη χρονική στιγμή ως το νέο επικεφαλής, υπολογίζει την τρέχουσα και την προβλεπόμενη μελλοντική εναπομένουσα ενέργεια των κόμβων μαζί με τον αριθμό των γύρων που μπορεί να είναι επικεφαλής συμπλέγματος, προκειμένου να μεγιστοποιηθεί η διάρκεια ζωής του δικτύου. Το δίκτυο μοντελοποιείται ως ένα γραμμικό σύστημα, και χρησιμοποιείται ο αλγόριθμος Gauss για να υπολογίσει τον συνδυασμό των κόμβων που μπορούν να επιλεγούν ως επικεφαλής συμπλέγματος. [213]

GEAR

Το πρωτόκολλο Επίγνωσης της Θέσης και της Ενέργειας είναι πρωτόκολλο βασισμένο στην Τοπολογία του δικτύου (Topology Based). Σε αντίθεση με τα προηγούμενα πρωτόκολλα, το GEAR δεν χρησιμοποιεί άπληστους αλγόριθμους για να προωθήσει το πακέτο στον προορισμό. Το GEAR χρησιμοποιεί την ενέργεια για να ενημερώσει τους γείτονες για την δρομολόγηση ενός πακέτου προς την περιοχή στόχο. Δύο κύρια χαρακτηριστικά αυτού του πρωτοκόλλου είναι τα ακόλουθα:

- Όταν υπάρχει κοντινός γείτονας στον προορισμό, το GEAR επιλέγει τον κόμβο μεταξύ των γειτόνων που είναι πιο κοντά στον προορισμό του.
- Όταν όλοι οι γείτονες είναι μακριά, το GEAR επιλέγει τον κόμβο που ελαχιστοποιεί το κόστος του γείτονα.

Το κύριο πλεονέκτημα του GEAR είναι ότι κάθε κόμβος γνωρίζει τη θέση και το υπολειπόμενο επίπεδο της ενέργειάς του, τις θέσεις του και τα υπόλοιπα των επιπέδων ενέργειας των γειτονικών κόμβων. Επίσης προσπαθεί να εξισορροπήσει την κατανάλωση ενέργειας και, ως εκ τούτου, να επεκτείνει τη διάρκεια ζωής του δικτύου [202].

Κεφάλαιο 4: Εργαλεία Υλοποίησης και Προσομοίωσης Σεναρίου [50]

Cisco Packet Tracer 7.2 [50]

Αυτό το κεφάλαιο κάνει μια επισκόπηση των εργαλείων που χρησιμοποιήθηκαν για την υλοποίηση των σεναρίων της εργασίας. Το βασικό εργαλείο ήταν το Cisco Packet Tracer 7.2. Το Packet Tracer έχει σχεδιαστεί από τη Cisco Systems και είναι ένα λογισμικό προσομοίωσης, το οποίο επιτρέπει στους χρήστες να δημιουργούν εικονικές τοπολογίες δικτύων ώστε να μπορούν να τις δουλεύουν σαν να είχαν πραγματικά δίκτυα υπολογιστών και τα αντίστοιχα πρωτόκολλα.

Το Packet Tracer μπορεί να προσομοιώσει μικρά έως αρκετά μεγάλα δίκτυα τα οποία μπορούν να αλληλεπιδρούν μεταξύ τους σε πραγματικό χρόνο. Πολύ εύκολα στο γραφικό του περιβάλλον δημιουργούμε τις συσκευές του δικτύου που θέλουμε να δοκιμάσουμε και τις παραμετροποιούμε. Δημιουργούμε για παράδειγμα ένα ή περισσότερα PCs ή laptops τα οποία εξοπλίζουμε με κατάλληλο υλικό (όπως ασύρματη ή ενσύρματη ή ακόμα και dial-up σύνδεση, θύρες USB, κλπ) και κάνουμε τις διαδικτυακές ρυθμίσεις (διευθύνσεις IP, μάσκα υποδικτύου, DNS server, κλπ) όπως ακριβώς θα κάναμε και με ένα πραγματικό PC. Με ανάλογο τρόπο εξοπλίζουμε και ρυθμίζουμε τους μεταγωγείς (switches), τους δρομολογητές (routers), και τους εξυπηρετητές (servers). Οι εξυπηρετητές μπορούν να ρυθμιστούν ώστε να υποστηρίζουν διάφορες υπηρεσίες (services, όπως FTP, HTTP, DNS, DHCP, Firewall κλπ). Την καλωδίωση μεταξύ των συσκευών μπορούμε να την επιλέξουμε ή να την αποφασίσει το σύστημα αυτόματα. Το Packet Tracer επιτρέπει τη προσομοίωση διεπαφής γραμμής εντολών (CLI, με περιορισμένο όμως αριθμό εντολών) για την διαμόρφωση των δρομολογητών (routers) και των μεταγωγέων (switches), δηλαδή την χρήση του IOS της Cisco. Αφού "εγκατασταθούν" και ρυθμιστούν οι συσκευές μπορούν να αρχίσουν οι δοκιμές σε τμήματα του δικτύου και να επεκταθούν στο σύνολό του. Οι δοκιμές γίνονται σε πραγματικό χρόνο με τα μέρη του δικτύου να ανταλλάσσουν πακέτα δεδομένων στα πλαίσια των λειτουργιών που τους έχουμε αναθέσει. Όταν παρουσιαστεί κάποιο πρόβλημα στο δίκτυο τότε το Packet Tracer μας δίνει την δυνατότητα να

παρακολουθήσουμε την διακίνηση των πακέτων βήμα - βήμα στην περιοχή που παρουσιάστηκε το σφάλμα. Μπορούμε να εξετάσουμε τη δρομολόγηση και τη δομή των πακέτων σχεδόν σε κάθε δυνατή λεπτομέρεια. Εξάλλου βασίζεται στο μοντέλο αναφοράς OSI και τα αντίστοιχα πρωτόκολλα.

Το Packet Tracer υλοποιήθηκε από τον Dennis Frezzo και την ομάδα του στη Cisco Systems για τη διευκόλυνση στην εκπαίδευση των σπουδαστών.

Λειτουργεί σε πλατφόρμες όπως Windows, Linux, MAC OS και διαθέτει παραπλήσια έκδοση σε κινητές συσκευές Android και iOS. Επίσης, τέσσερις τύποι προβλημάτων υποστηρίζονται καλά από το Packet Tracer:

- Concept-builders: απαιτήσεις σχεδίασης δικτυακών μοντέλων που οδηγούν σε εξηγήσεις που δημιουργούν οι σπουδαστές και προσομοιώσεις εννοιών δικτύωσης
- Skill-builders: αλγοριθμική επίλυση προβλημάτων για την υποστήριξη της ανάπτυξης διαδικαστικών γνώσεων δικτύωσης
- Design challenges: προβλήματα βασισμένα σε περιορισμούς με πολλαπλές σωστές λύσεις
- Troubleshooting challenges: διάγνωση, απομόνωση και αποκατάσταση του προσομοιωμένου δικτύου από ένα αρχείο δικτύου που προηγουμένως είχε διαγνωσθεί από τον σπουδαστή ότι περιέχει σφάλματα

Το Packet Tracer προσφέρει ασκήσεις για περίπου το 80% των θεμάτων και δεξιοτήτων που απαιτούνται για τις πιστοποιήσεις CCNA, CCNA-Security, CCNP, IT Essentials και γενικά μαθήματα σε TCP/IP.

Παρέχει δύο *χώρους εργασίας* :

- Ο *Λογικός Χώρος Εργασίας* (Logical Workspace). Εδώ μας ενδιαφέρει η παραμετροποίηση του δικτύου και θέλουμε να είναι όσο γίνεται πιο κατανοητή οπτικά. Παρέχεται πληθώρα δικτυακών πρωτοκόλλων
- Ο *Φυσικός Χώρος Εργασίας* (Physical Workspace) στον οποίο τοποθετούμε στις πραγματικές τους θέσεις τα μέρη του δικτύου μας. Έχουμε μια κάτοψη του χώρου όπου σε ειδικό δωμάτιο έχουμε τις σημαντικές δικτυακές συσκευές (εξυπηρετητές, δρομολογητές, κλπ) και στους υπόλοιπους χώρους, στις θέσεις εργασίας τα PCs, εκτυπωτές, κλπ. Ο βασικός σκοπός, είναι ο έλεγχος της αξιοπιστίας του δικτύου που σχεδιάζουμε στον πραγματικό του χώρο

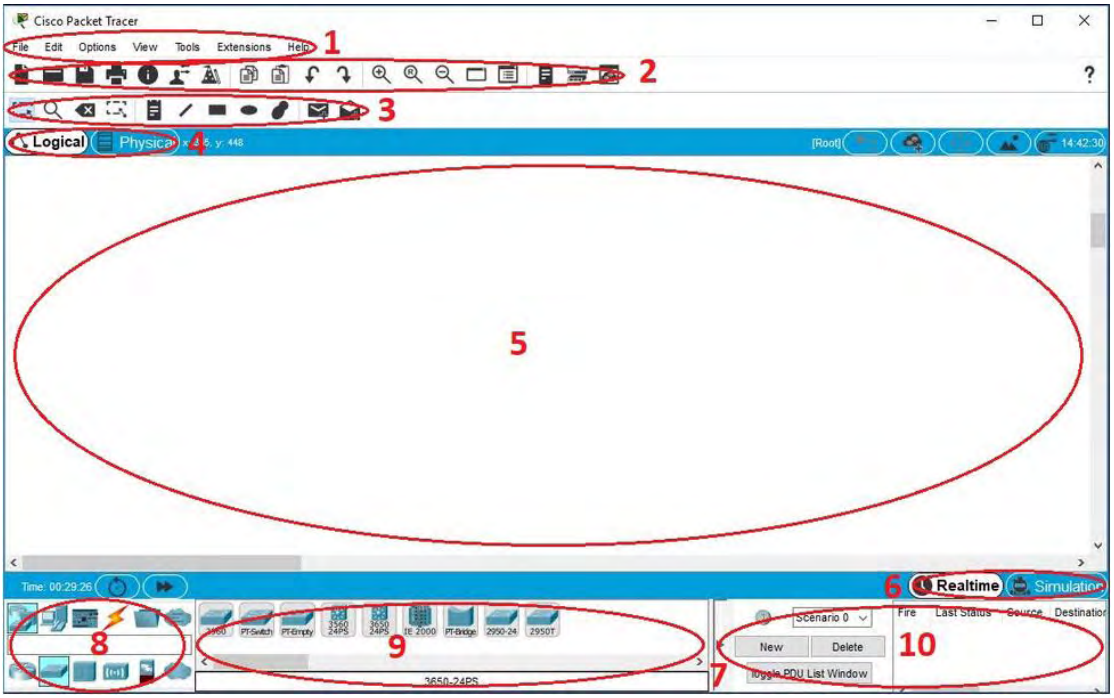
Ακόμα έχουμε δύο *καταστάσεις λειτουργίας* :

- *Πραγματικού χρόνου* (Real Time Mode) όπου το δίκτυο κάνει προσομοίωση σε πραγματικές συνθήκες όσον αφορά τον όγκο των πληροφοριών, τον χρόνο μετάδοσης, κλπ.
- *Προσομοίωσης* (Simulation Mode) όπου ελέγχουμε βήμα βήμα τη λειτουργία του δικτύου για να εντοπίσουμε σφάλματα, αλλά και για να αναλύσουμε την όλη διαδικασία σε κάθε λεπτομέρεια της.

Το *εικονικό υλικό* (hardware) περιλαμβάνει :

- *Δικτυακές συσκευές* (μεταγωγείς, δρομολογητές, κλπ) που αποτελούνται από δομοστοιχεία και μπορούν να τροποποιηθούν (modular devices) σε γραφικό περιβάλλον (GUI). Εκτός από τις κοινές συσκευές έχουμε IP τηλέφωνα, VOIP συσκευές, TVs, κλπ.
- *Καλωδίωση* κάθε είδους, Ethernet , ομοαξονικά, τηλεφωνικά , οπτικές ίνες, κλπ.

Επίσης υπάρχει κ η δυνατότητα λειτουργίας *πολλών χρηστών* (multiuser) που μπορούν να εργάζονται σε τμήματα του ίδιου εικονικού δικτύου.
Για την εξοικείωση του χρήστη το Packet Tracer συνοδεύεται με εμπεριστατωμένη Βοήθεια (Help) και εκπαιδευτικό υλικό (tutorial).



Το default περιβάλλον του Packet Tracer [222]

1	Menu Bar	Αυτή η γραμμή περιέχει τα μενού: Αρχείο, Επεξεργασία, Επιλογές, Προβολή, Εργαλεία, Επεκτάσεις και Βοήθεια. Εκεί βρίσκονται βασικές εντολές, όπως Άνοιγμα, Αποθήκευση, Αποθήκευση ως Pkz, Εκτύπωση και Ρυθμίσεις και Προτιμήσεις σε αυτά τα μενού. Επίσης υπάρχει η δυνατότητα πρόσβασης στον Activity Wizard από το μενού Επεκτάσεις.
2	Main Tool Bar	Αυτή η γραμμή παρέχει εικονίδια συντόμευσης στις πιο συχνά χρησιμοποιούμενες εντολές μενού.
3	Common Tools Bar	Αυτή η γραμμή παρέχει πρόσβαση στα συνήθως χρησιμοποιούμενα εργαλεία χώρου εργασίας: Επιλογή, Επιθεώρηση, Διαγραφή, Αλλαγή μεγέθους σχήματος, Σημείωση θέσης, Παλέτα σχεδίασης, Προσθήκη απλού PDU και Προσθήκη σύνθετου PDU.
4	Logical/Physical Workspace and Navigation Bar	Μπορούμε να μεταβούμε μεταξύ του Φυσικού και του Λογικού χώρου εργασίας με τις καρτέλες αυτής της γραμμής. Στον Λογικό Χώρο Εργασίας, αυτή η μπάρα μας επιτρέπει επίσης να επιστρέψουμε σε ένα προηγούμενο επίπεδο σε ένα cluster, να δημιουργήσετε ένα νέο cluster, Μετακίνηση Αντικειμένου, Ρύθμιση φόντου και Viewport. Στον Φυσικό Χώρο Εργασίας, αυτή η μπάρα μας επιτρέπει να περιηγηθούμε σε φυσικές τοποθεσίες, να δημιουργήσουμε μια Νέα Πόλη, ένα Νέο Κτίριο, ένα Νέο

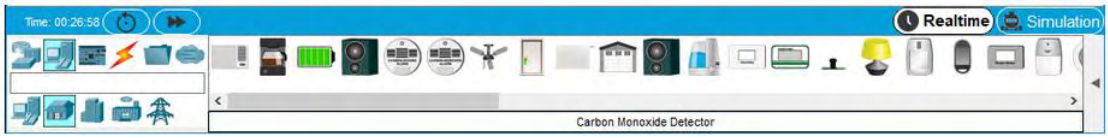
		Closet, να Μετακινήσετε Αντικείμενο, να χρησιμοποιήσουμε ένα μια εικόνα για φόντο, να ορίσουμε Ιστορικό και να πάμε στο Working Closet.
5	Workspace	Αυτή η περιοχή είναι όπου θα δημιουργήσουμε το δίκτυο μας, θα παρακολουθήσουμε προσομοιώσεις και θα δούμε πολλά είδη πληροφοριών και στατιστικών
6	Realtime/Simulation Bar	Μπορούμε να μεταβούμε μεταξύ της λειτουργίας πραγματικού χρόνου και της λειτουργίας προσομοίωσης με τις καρτέλες σε αυτήν τη γραμμή. Αυτή η μπάρα παρέχει επίσης κουμπιά Power Cycle Devices και Fast Forward Time, καθώς και τα κουμπιά ελέγχου αναπαραγωγής και το κουμπί εναλλαγής της λίστας συμβάντων στη λειτουργία προσομοίωσης. Επίσης, περιέχει ένα ρολόι που εμφανίζει το σχετικό χρόνο στις καταστάσεις λειτουργίας πραγματικού χρόνου και προσομοίωσης.
7	Network Component Box	Αυτό το πλαίσιο είναι εκεί όπου επιλέγουμε συσκευές και συνδέσεις για να τις τοποθετήσουμε στο χώρο εργασίας. Περιέχει το πλαίσιο επιλογής συσκευής και το πλαίσιο επιλογής συγκεκριμένης συσκευής. Υπάρχει ένα πεδίο με δυνατότητα αναζήτησης που σας επιτρέπει να εισάγετε ένα όνομα συσκευής για να αναζητήσετε γρήγορα τη συγκεκριμένη συσκευή. Το όνομα της συσκευής εμφανίζεται όταν αφήνουμε το ποντίκι πάνω από το εικονίδιο της συσκευής στο πλαίσιο Device-Specific Box
8	Device-Type Selection Box	Αυτό το πλαίσιο περιέχει τον τύπο συσκευών και τις συνδέσεις που είναι διαθέσιμες στο Packet Tracer. Το Device-Type Selection Box θα αλλάξει ανάλογα με τον τύπο συσκευής που θα επιλέξουμε.
9	Device-Specific Selection Box	Σε αυτό το πλαίσιο επιλέγουμε συγκεκριμένα τις συσκευές που θέλουμε να τοποθετήσουμε στο δίκτυο μας και ποιες συνδέσεις πρέπει να κάνουμε. Σε αυτό το πλαίσιο, μπορεί να βρούμε συσκευές που να είναι ήδη ξεπερασμένες. Έχουμε την επιλογή να αποκρύψουμε τον παλαιό εξοπλισμό στο παράθυρο "Προτιμήσεις" στην καρτέλα Επιλογές.
10	User Created Packet Window*	Αυτό το παράθυρο διαχειρίζεται τα πακέτα που τοποθετούμε στο δίκτυο κατά τη διάρκεια των σεναρίων προσομοίωσης.

Η Cisco δημιούργησε το Packet Tracer για να χρησιμοποιηθεί σαν συμπληρωματικό βοήθημα για τους σπουδαστές της είτε είναι στην αίθουσα διδασκαλίας είτε μελετούν μόνοι τους. Με τη βοήθεια του, οι εκπαιδευτές μπορούν να παρουσιάσουν περίπλοκες τεχνικές έννοιες. Μπορούν να συνθέσουν, να πειραματιστούν, να εκτελέσουν προμελετημένα σενάρια και να εντοπίσουν σφάλματα σε ένα περίπλοκο εικονικό δίκτυο σε λιγότερο χρόνο σε σχέση με ένα πραγματικό δίκτυο. Η προσομοίωση διευκολύνει την παρουσίαση εσωτερικών λειτουργιών του δικτύου και την ανάλυση της δρομολόγησης των δεδομένων ακριβώς την στιγμή που συμβαίνει, πράγμα που θα ήταν δύσκολο σε πραγματικές συνθήκες (real time). Οι σπουδαστές όταν μελετούν μόνοι τους έχουν στη διάθεση τους την λειτουργικότητα πλήθους πανάκριβων μηχανημάτων και την ευχέρεια κάθε πειραματισμού χωρίς τον κίνδυνο να προκαλέσουν ζημιά.

Μάλιστα το Packet Tracer τους εκπαιδεύει στο να είναι προσεκτικοί. Δεν τους επιτρέπει να αλλάζουν εξαρτήματα σε αναμμένη συσκευή έστω και αν είναι εικονική! Πρέπει πρώτα να την σβήσουν "εικονικά"! [49]

Εκτός από τις κλασικές συσκευές δικτύου που υπάρχουν σε παλαιότερες εκδόσεις του Packet Tracer, το Packet Tracer 7.1.1 περιλαμβάνει μια μεγάλη ποικιλία από «έξυπνες» συσκευές (smart things) και εξαρτήματα (components):

Smart Things, είναι φυσικά αντικείμενα που μπορούν να συνδεθούν στον Εξυπηρετητή Εγγραφής (Registration Server) ή στην Οικιακή πύλη δικτύου (Home Gateway) μέσω μια δικτυακής διεπαφής (network interface). Διαχωρίζονται σε υποκατηγορίες κάτω από την καρτέλα End Devices. Οι κατηγορίες αποτελούνται από το Home, Smart City, Industrial και Power Grid. Παρακάτω φαίνονται μερικές συσκευές Smart Thing της κατηγορίας Home.



Smart Things [222]

Components, είναι φυσικά αντικείμενα τα οποία συνδέονται είτε σε μικροελεγκτές (MCU-PT) είτε σε Single Boarded Computers (SBC-PT). Είναι απλές συσκευές που επικοινωνούν μόνο μέσω των αναλογικών ή ψηφιακών υποδοχών τους με τα MCU-PT και SBC-PT για να συνδεθούν στο δίκτυο καθώς τα ίδια δεν διαθέτουν δικτυακή διεπαφή.

Επίσης, υπάρχουν ακόμη τρείς υποκατηγορίες για τα Components:

- Πλακέτες (Boards): μικροελεγκτές (MCU-PT), Single Boarded Computers (SBC-PT) και μια ειδική συσκευή που ονομάζεται Thing, η οποία χρησιμοποιείται για τη δημιουργία αυτόνομων φυσικών αντικειμένων όπως καφετιέρες και συναγερμοί καπνού.
- Ενεργοποιητές (Actuators): Αυτά τα εξαρτήματα χειρίζονται το περιβάλλον, τον εαυτό τους, ή τον χώρο γύρω τους, για παράδειγμα LED, συσκευές καταιονισμού κ.λ.π.
- Αισθητήρες (Sensors): Αυτά τα εξαρτήματα «αισθάνονται/νιώθουν» το περιβάλλον (αισθητήρες φωτός, αισθητήρες θερμοκρασίας), τον χώρο γύρω τους (RFID, ανιχνευτές μετάλλου) ή τις αλληλεπιδράσεις (ποτενσιόμετρο, πιεζόμενο κουμπί)

Παρακάτω είναι μια εικόνα με μερικά components αισθητήρων:

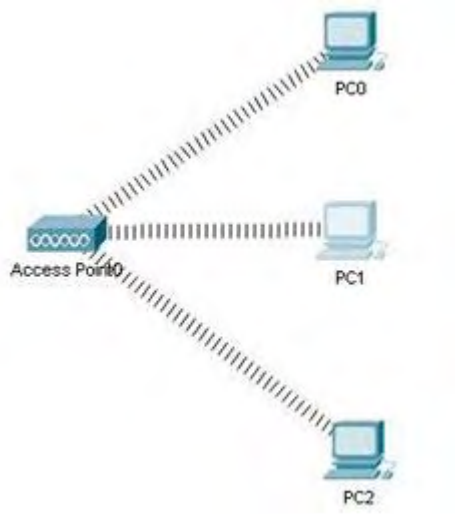
Sensor Components [222]

Το Packet Tracer υποστηρίζει ένα ευρύ φάσμα συνδέσεων δικτύου. Κάθε τύπος καλωδίου μπορεί να συνδεθεί μόνο σε συγκεκριμένους τύπους διεπαφών.

Είδος καλωδίου	*Περιγραφή*
Console	Οι συνδέσεις τύπου console μπορούν να γίνουν μεταξύ υπολογιστών και router ή switch. Πρέπει να πληρούνται ορισμένες προϋποθέσεις για να λειτουργήσει η σύνδεση console

	από τον υπολογιστή: η ταχύτητα και στις δύο πλευρές της σύνδεσης πρέπει να είναι ίδια, τα data bits πρέπει να είναι 7 ή 8 και για τις δύο πλευρές, η ισοτιμία πρέπει να είναι ίδια, τα stop bits πρέπει να είναι 1 ή 2 (αλλά δεν χρειάζεται να είναι τα ίδια και για τις δύο πλευρές) και ο έλεγχος ροής μπορεί να μην είναι ο ίδιος και για τις δύο πλευρές.
 **Copper Straight-through**	Αυτός ο τύπος καλωδίου είναι το κλασικό καλώδιο Ethernet για σύνδεση μεταξύ συσκευών που λειτουργούν σε διαφορετικά επίπεδα OSI (όπως hub με router και switch με υπολογιστή). Μπορεί να συνδεθεί στους ακόλουθους τύπους θυρών: 10 Mbps Copper (Ethernet), 100 Mbps Copper (Fast Ethernet) και 1000 Mbps Copper (Gigabit Ethernet).
 **Copper Cross-over**	Αυτός ο τύπος καλωδίου είναι επίσης το κλασικό καλώδιο Ethernet για σύνδεση όμως μεταξύ συσκευών που λειτουργούν στο ίδιο στρώμα OSI (όπως hub με hub, PC με PC, PC με εκτυπωτή). Μπορεί να συνδεθεί στους ακόλουθους τύπους θυρών: 10 Mbps Copper (Ethernet), 100 Mbps Copper (Fast Ethernet) και 1000 Mbps Copper (Gigabit Ethernet).
 **Fiber**	Οι οπτικές ίνες χρησιμοποιούνται για τη δημιουργία συνδέσεων μεταξύ θυρών για οπτικές ίνες (100 Mbps ή 1000 Mbps).
 **Phone**	Οι συνδέσεις τηλεφωνικής γραμμής μπορούν να πραγματοποιηθούν μόνο μεταξύ συσκευών με θύρες για μόντεμ. Η τυπική εφαρμογή για συνδέσεις μόντεμ είναι μια end device (όπως PC) που καταλήγει σε ένα cloud δικτύου.
 **Coaxial**	Τα ομοαξονικά μέσα χρησιμοποιούνται για τη δημιουργία συνδέσεων μεταξύ ομοαξονικών θυρών, όπως ένα καλωδιακό μόντεμ συνδεδεμένο σε Packet Tracer Cloud.
 **Serial DCE και DTE**	Οι σειριακές συνδέσεις, που χρησιμοποιούνται συχνά για συνδέσεις WAN, πρέπει να συνδέονται μεταξύ των σειριακών θυρών. Να ληφθεί υπόψη ότι πρέπει να ενεργοποιήσετε το clocking στην πλευρά DCE για να ενεργοποιηθεί το πρωτόκολλο. Το DTE clocking είναι προαιρετικό. Μπορείτε να καταλάβουμε ποιο άκρο της σύνδεσης είναι η πλευρά DCE από το μικρό εικονίδιο "ρολόι" δίπλα στη θύρα. Εάν επιλέξουμε τον τύπο σύνδεσης Serial DCE και, στη συνέχεια, συνδέσετε δύο συσκευές, η πρώτη συσκευή θα είναι η πλευρά DCE και η δεύτερη συσκευή θα ρυθμιστεί αυτόματα στην πλευρά DTE. Το αντίστροφο ισχύει αν επιλέξουμε τον τύπο σύνδεσης Serial DTE.
 **Octal**	Το ασύγχρονο καλώδιο 8 θυρών παρέχει την υποδοχή υψηλής πυκνότητας στο ένα άκρο και οκτώ βύσματα RJ-45 στο άλλο.
 **IoE Custom Cable**	Ένα καλώδιο για τη σύνδεση των things, των component, των μικροελεγκτών (MCU-PT) και των υπολογιστών (SBC-PT). Το καλώδιο συνδέει τα καλώδια γείωσης, τροφοδοσίας και δεδομένων.
 **USB**	Το καλώδιο USB χρησιμοποιείται για τη σύνδεση των things, των component, των μικροελεγκτών (MCU-PT) και των υπολογιστών (SBC-PT) ως σύνδεση δεδομένων.

Επίσης, μπορούμε να δημιουργήσουμε και ασύρματες συνδέσεις μεταξύ σημείων πρόσβασης και τελικών συσκευών (υπολογιστές, διακομιστές και εκτυπωτές). Για να δημιουργήσουμε μια ασύρματη σύνδεση, απλώς αφαιρούμε την υπάρχουσα υποδοχή σε μια τελική συσκευή, τοποθετούμε την ασύρματη και ενεργοποιούμε τη συσκευή. Η συσκευή θα προσπαθήσει αυτόματα να συσχετιστεί με ένα σημείο πρόσβασης. Συνήθως, αυτό σημαίνει ότι θα συνδεθεί (φυσικά) με το πλησιέστερο σημείο πρόσβασης. [222]

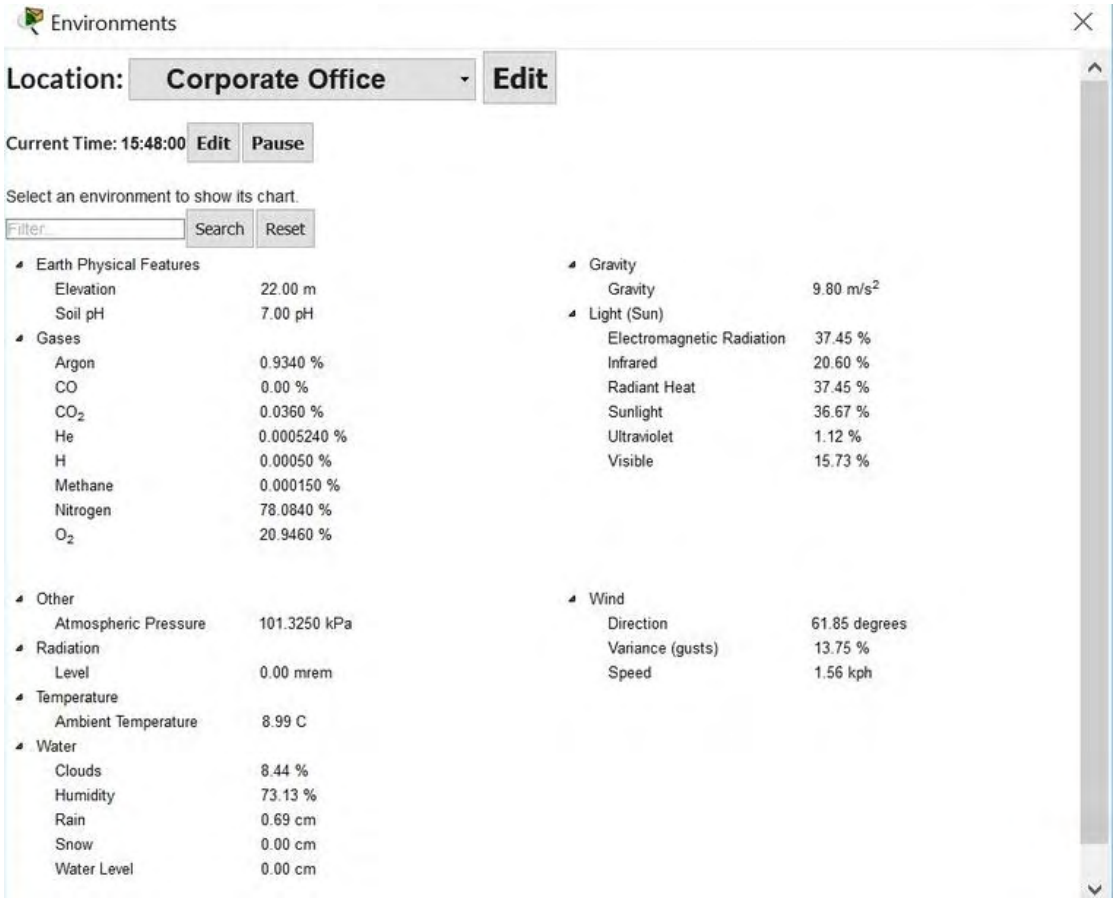


Παράδειγμα ασύρματης σύνδεσης τερματικών συσκευών και ασύρματου σημείου πρόσβασης [222]

Επιπλέον, τα intercity, city, buildings, wiring closets, και generic containers έχουν όλα ένα περιβάλλον. Υπάρχουν μερικές δωδεκάδες προεπιλεγμένα περιβάλλοντα, όπως θερμοκρασία, βροχή, στάθμη νερού, ταχύτητα ανέμου και χιόνι. Όταν οι συσκευές δεν επηρεάζουν το περιβάλλον, οι τιμές τους κυμαίνονται σε έναν κύκλο 24 ωρών. Για παράδειγμα, ο ήλιος θα βγει στις 6 το πρωί και θα βασιλέψει στις 6μμ. Η θερμοκρασία περιβάλλοντος θα κορυφωθεί στους 25 ° C το μεσημέρι. Αυτός ο κύκλος είναι ρυθμισμένος στο intercity επίπεδο και η περιοχή θερμοκρασίας περιβάλλοντος αναμεταδίδεται αυτόματα στην κεντρική wiring closet. Αν μια θερμαντική συσκευή προστεθεί στο Corporate Office και ενεργοποιηθεί, η θερμοκρασία μέσα στο Corporate Office θα αυξηθεί μαζί με όλα τα container μέσα σε αυτό. Να σημειωθεί, ωστόσο, ότι ο θερμαντήρας δεν θερμαίνει το parent container, δηλαδή το Home City, αλλά θερμαίνει μόνο τα child container. Όταν ο θερμαντήρας είναι απενεργοποιημένος, το Corporate Office τελικά θα συγκλίνει στη θερμοκρασία περιβάλλοντος του parent container, δηλαδή του Home City, με βάση τους δικούς του ρυθμούς μεταβίβασης θερμοκρασίας. Τα διαφορετικά container μπορεί να έχουν διαφορετικά επίπεδα μόνωσης και έτσι διαφορετικούς ρυθμούς μεταβίβασης θερμοκρασίας. Ο ρυθμός μεταβίβασης θερμοκρασίας καθορίζει την ταχύτητα που συγκλίνει το child container με το parent container και λειτουργεί με τον ίδιο τρόπο για όλους τους τύπους περιβάλλοντος.

Πολλές συσκευές ή πράγματα επηρεάζουν ή ανταποκρίνονται στο περιβάλλον με κάποιο τρόπο. Ένας πυροσβεστήρας θα αυξήσει τη στάθμη και την υγρασία του νερού σε ένα container. Ένα παλιό αυτοκίνητο θα αυξήσει το διοξείδιο του άνθρακα και τη θερμοκρασία

περιβάλλοντος όταν το θέσουμε σε λειτουργία. Ένας ανιχνευτής καπνού μπορεί να χρησιμοποιηθεί για να προκαλέσει τον συναγερμό όταν ο καπνός στο περιβάλλον αυξηθεί πάνω από ένα συγκεκριμένο όριο. Ένα πλήρες φάσμα συσκευών και πραγμάτων που ανταποκρίνονται και επηρεάζουν το περιβάλλον παρατίθενται παρακάτω. [222]



Το Environment Dialog μας επιτρέπει να προβάλουμε και να επεξεργαστούμε το περιβάλλον μέσα στο φυσικό container [222]

Ο παρακάτω κατάλογος απαριθμεί τις IoT συσκευές του Packet Tracer 7.1 και τη συμπεριφορά τους ανάλογα με το περιβάλλον προσομοίωσης στο οποίο βρίσκονται.

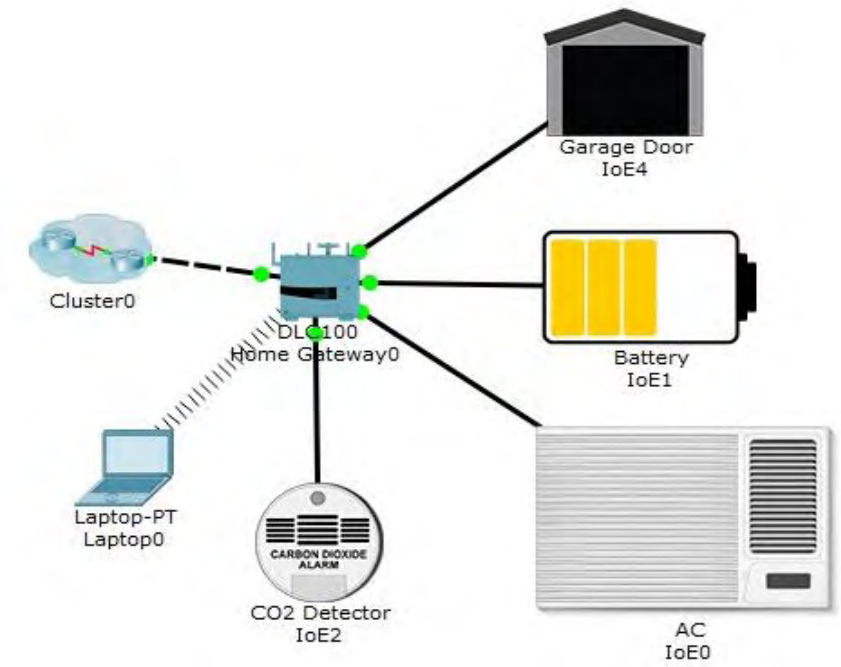
Thing	*Icon*	*Environment Behavior*
ATM Pressure Sensor		Detects the Atmospheric Pressure and displays it. The default detection range is from 0 to 110 kPa.
Carbon Dioxide Detector		Detects Carbon Dioxide.
Carbon Monoxide Detector		Detects Carbon Monoxide.
Door		Affects Argon, Carbon Monoxide, Carbon Dioxide, Hydrogen, Helium, Methane, Nitrogen, O2, Ozone, Propane, and Smoke. When the door is opened, those gases will decrease to a maximum of 2% in total change.
Fan		Affects Wind Speed, Humidity, and Ambient Temperature. At Low Speed Setting, the Wind Speed is set to 0.4 kph. The rate of cooling the Ambient Temperature is set to -1C/hour. The rate of reducing the Humidity is set to -1% per hour. At High Speed Setting, the Wind Speed is set to 0.8 kph. The rates of change for Ambient Temperature and Humidity is two times of the low setting.
Fire Sprinkler, Ceiling Sprinkler		Affects Water Level at a rate of 0.1 cm per second. Affects Humidity at a rate of 5% per hour.
Garage Door		Affects Argon, Carbon Monoxide, Carbon Dioxide, Hydrogen, Helium, Methane, Nitrogen, O2, Ozone, Propane, and Smoke. When the door is opened, those gases will decrease to a maximum of 4% in total change. When the door is opened, the rate of transference for Humidity and Temperature is increased by 50%. The rate of transference for gases is increased by 100%.
Home Speaker, Speaker		Affects Sound Volume at 65 dB. Affects Sound Pitch at 20 CPS to 60 CPS. Affects White Noise at 20%.

Humidifier		Affects Humidity at a rate of 1% per hour.
Humidity Sensor		Detects Humidity.
Humiture Monitor, Humiture Sensor		Detects Ambient Temperature and Humidity and outputs the value as a sum of the Ambient Temperature and Humidity divided by 2.
Lawn Sprinkler, Floor Sprinkler		Affects Water Level at a rate of 0.1 cm per second. Affects Humidity at a rate of 5% per hour.
LED		Affects Visible Light with a maximum output of 1%.
Light		Affects Visible Light with a maximum output of 20%.
Old Car		Affects Carbon Monoxide at a rate of 1% per hour. Affects Carbon Dioxide at a rate of 2% per hour. Affects Smoke at a rate of 3% per hour. Affects Ambient Temperature at a rate of 1% per hour.
Photo Sensor		Detects Visible Light.
Piezo Speaker		Affects Sound Volume at 10 dB. Affects Sound Pitch 20 CPS.
RGB LED		Affects Visible Light with a maximum output of 2%.
Smart LED, Dimmable LED		Affects Visible Light with a maximum output of 3%.
Smoke Detector, Smoke Sensor		Detects Smoke.

Solar Panel		Detects Sunlight to generate electricity.
Temperature Monitor		Detects Ambient Temperature.
Temperature Sensor		Detects Ambient Temperature.
Water Level Monitor, Water Detector		Detects Water Level.
Wind Sensor		Detects Wind Speed.
Wind Turbine		Detects Wind Speed to generate electricity.
Window		Affects Argon, Carbon Monoxide, Carbon Dioxide, Hydrogen, Helium, Methane, Nitrogen, O2, Ozone, Propane, and Smoke. When the door is opened, those gases will decrease to a maximum of 1% in total change. When the door is opened, the rate of transference for Humidity and Temperature is increased by 20%. The rate of transference for gases is increased by 100%.

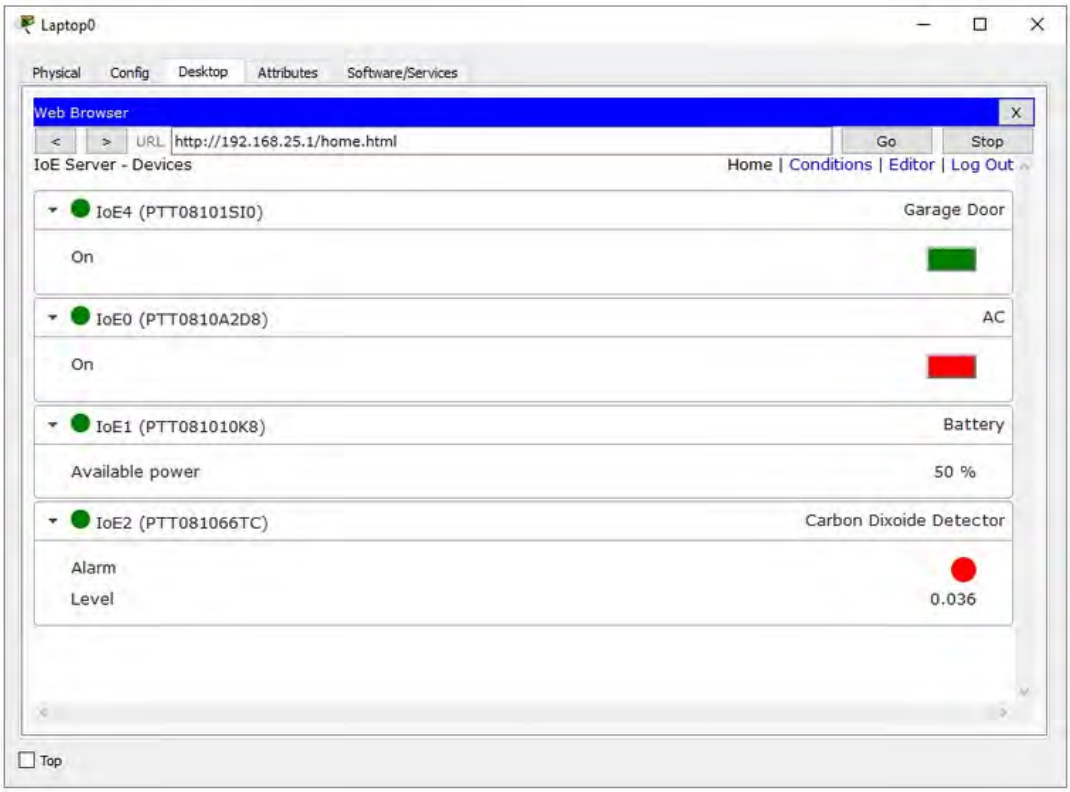
Οι IoT συσκευές του Packet Tracer και η λειτουργίες τους [50]

Το πρωτόκολλο MQTT έχει προστεθεί στο Packet Tracer 7.1 για τη βελτίωση της επικοινωνίας μεταξύ των IoT συσκευών. Οι έξυπνες συσκευές και εξαρτήματα (Things) μπορούν να συνδεθούν απευθείας στον Εξυπηρετητή Εγγραφής (Registration Server) ή σε έναν Εξυπηρετητή (Server) που όμως έχει ρυθμιστεί με τη λειτουργία του IoT service. Η οικιακή δικτυακή πύλη (home gateway) παρέχει 4 θύρες Ethernet αλλά και δυνατότητα για ασύρματη σύνδεση με όνομα δικτύου (SSID) για παράδειγμα “HomeGateway” στο κανάλι 6. Τα πρωτόκολλα WEP / WPA-PSK / WPA2 enterprise μπορούν να ρυθμιστούν για να παρέχουν ασφάλεια στις ασύρματες συνδέσεις. Η παρακάτω εικόνα δείχνει 4 «έξυπνες» συσκευές που είναι συνδεδεμένες σε μια οικιακή δικτυακή πύλη (home gateway) με την τελευταία να είναι συνδεδεμένη στο Ίντερνετ μέσω της θύρας WAN Ethernet.



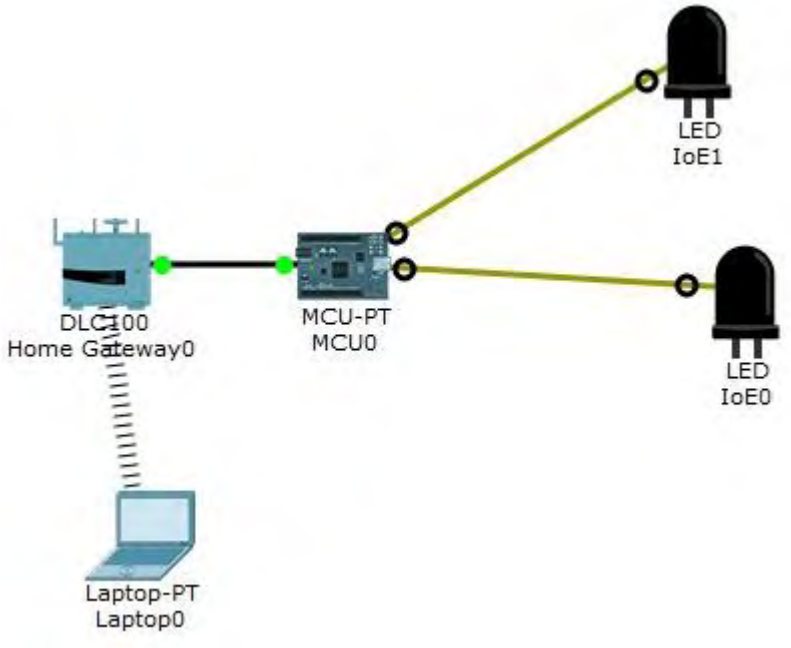
Προσομοίωση IoT δικτύου στο packet Tracer [50]

Οι «έξυπνες» συσκευές μπορούν να διαχειριστούν απομακρυσμένα μέσω μιας διεπαφής ιστού που παρέχεται από την οικιακή δικτυακή πύλη. Η παρακάτω εικόνα παρουσιάζει την κατάσταση των τεσσάρων «έξυπνων» συσκευών που είναι σε σύνδεση με την οικιακή δικτυακή πύλη.



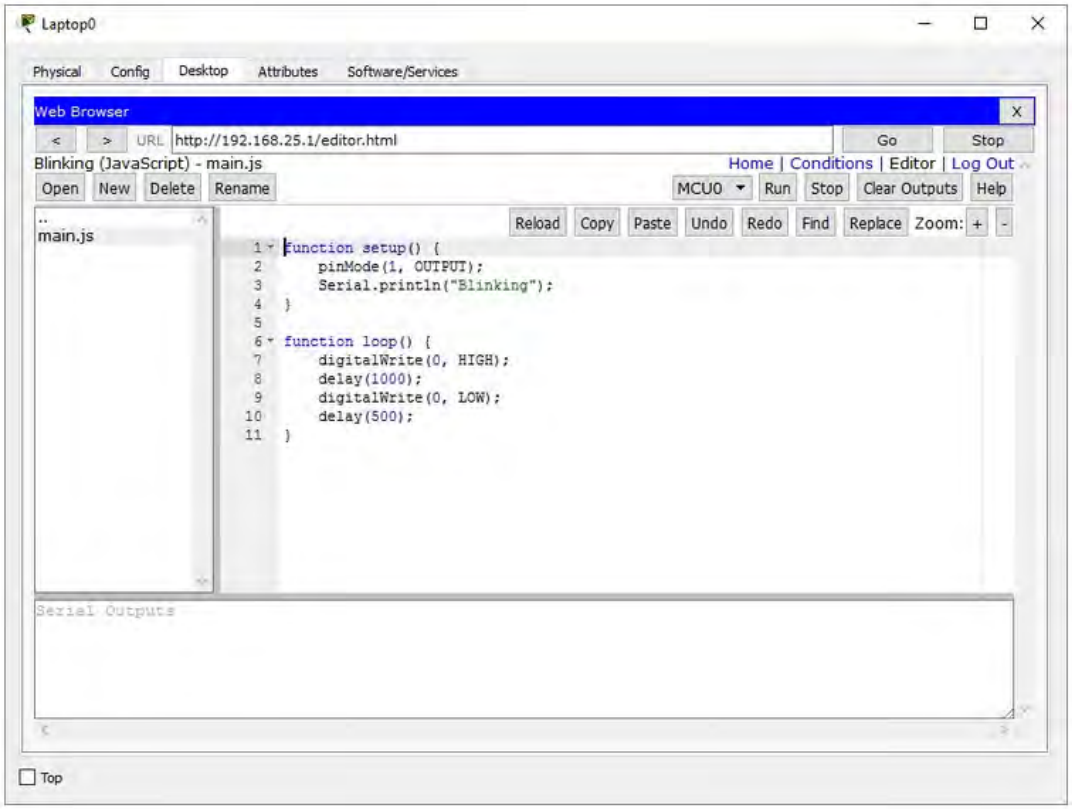
Διαχείριση διασυνδεδεμένων συσκευών από το laptop [50]

Όσων αφορά τα IoT εξαρτήματα (IoT components) του Packet Tracer 7.1.1 τα οποία δεν διαθέτουν διεπαφή Ethernet, δεν μπορούν να συνδεθούν απευθείας με την οικιακή δικτυακή πύλη. Οι αισθητήρες και οι ενεργοποιητές που ανήκουν στα εξαρτήματα, μπορούν να συνδεθούν σε μικροελεγκτές (MCU-PT). Ο μικροελεγκτής (MCU-PT) συνδέεται στην οικιακή δικτυακή πύλη η οποία βλέπει τον μικροελεγκτή αλλά όχι τα IoT εξαρτήματα που είναι συνδεδεμένα σε αυτόν. Η οικιακή δικτυακή πύλη με τη σειρά της βασίζεται στον απομακρυσμένο έλεγχο των IoT εξαρτημάτων μέσω της Διεπαφής Προγραμματισμού Εφαρμογών (API) όπως έχει προγραμματιστεί στον μικροελεγκτή.



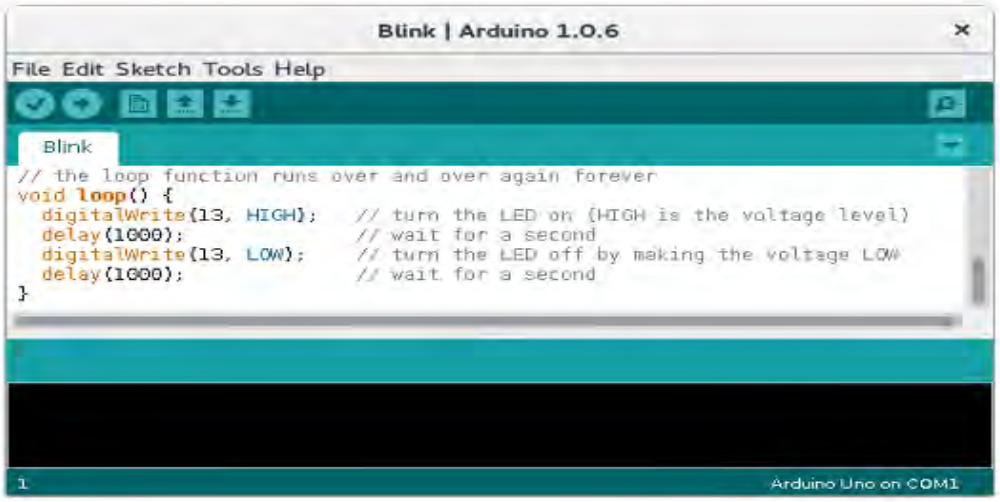
Απλό παράδειγμα στο Packet Tracer με τον μικροελεγκτή [50]

Τέλος, οι πραγματικές πλακέτες μικροελεγκτών είναι για παράδειγμα οι πλακέτες Arduino όπως το Arduino Yún Shield. Η οικιακή δικτυακή πύλη διαθέτει πρόγραμμα επεξεργασίας κώδικα στη διεπαφή ιστού για τον προγραμματισμό των IoT εξαρτημάτων. Συγκεκριμένα, για τον προγραμματισμό του μικροελεγκτή (MCU-PT) οι γλώσσες προγραμματισμού που αναγνωρίζονται είναι η JavaScript και η python. Ο κώδικας γράφεται μέσω της διεπαφής ιστού και μετά δημοσιεύεται στην πλακέτα MCU. Η παρακάτω εικόνα είναι ένα παράδειγμα προγραμματισμού της πλακέτας MCU σε JavaScript. Αυτός ο κώδικας, κάνει το ένα από τα δύο led της παραπάνω εικόνας να αναβοσβήνει.



Παράδειγμα προγραμματισμού της πλακέτας MCU σε JavaScript (Packet Tracer) [50]

Όπως φαίνεται από την παρακάτω εικόνα, το Packet Tracer 7.1.1 εξομοιώνει το Ολοκληρωμένο Περιβάλλον Ανάπτυξης (Integrated Development Environment) με το ακρωνύμιο IDE του Arduino, για τον προγραμματισμό των IoT αντικειμένων.



Το ίδιο παράδειγμα αλλά σε Arduino [50]

Κεφάλαιο 5: Υλοποίηση IoT Σεναρίου

5.1 Τεχνοοικονομική μελέτη

Ο όρος τεχνικοοικονομική μελέτη εκφράζει απόλυτα το σύγχρονο καθημερινό αντικείμενο δουλειάς του Επιστήμονα που εμπλέκεται στον Παραγωγικό Τομέα. Σημαίνει ότι κάθε τεχνική μελέτη πρέπει πάντα να συνοδεύεται και να ολοκληρώνεται από την αντίστοιχη μελέτη του οικονομικού της περιεχομένου που τελικά θα κρίνει εάν μπορεί να υλοποιηθεί και με ποια αποτελέσματα. Έτσι η τεχνοοικονομική μελέτη είναι απαραίτητη κατά την σχεδίαση μιας νέας μονάδας, την μετατροπή ή επέκταση υπάρχουσας μονάδας, την αγορά νέων μηχανημάτων ή αντικατάσταση παλαιών, την τήρηση αποθεμάτων πρώτων και βοηθητικών υλών, ανταλλακτικών και προϊόντων, την ανάπτυξη νέου προϊόντος ή βελτίωση υπάρχοντος, την ανάπτυξη νέας διεργασίας ή βελτίωση υπάρχουσας, την μετατροπή ενός αποβλήτου παραπροϊόντος σε πολύτιμο προϊόν, την εξοικονόμηση ενέργειας, την εφαρμογή μεθόδων εργασίας, κλπ. [165]

Το σενάριο της παρούσας διπλωματικής, αφορά την ανάθεση του σχεδιασμού και της υλοποίησης του δικτύου μιας έξυπνης κατοικίας για μια οικογένεια, σε έναν ιδιώτη (freelancer) μηχανικό δικτύων. Οι ανάγκες της οικογένειας αφορούν την ασφάλεια, την εξοικονόμηση ενέργειας, την άνεση και τον απομακρυσμένο και ασφαλή έλεγχο όλων των συστημάτων του σπιτιού. Με την κατάλληλη καλωδιακή υποδομή του κτιρίου δίνεται η δυνατότητα στο οικιακό περιβάλλον να ρυθμίζει αυτόματα όλα τα επιμέρους συστήματα σύμφωνα με τις προκαθορισμένες επιθυμίες του ιδιοκτήτη, μέσω της ενοποίησης όλων των περιφερειακών συστημάτων και εφαρμογών.

Σε αυτό το σημείο θα πραγματοποιηθεί η τεχνοοικονομική μελέτη της έξυπνης κατοικίας. Η παρακάτω κάτοψη αφορά ένα σπίτι 150 τ.μ με ένα υπνοδωμάτιο, μια κουζίνα, ένα μπάνιο, ένα καθιστικό και μια τραπεζαρία. Οι ιδιοκτήτες του είναι δύο και ζήτησαν να έχουν τον απόλυτο έλεγχο του σπιτιού τους όταν θα είναι εντός αλλά και εκτός της οικίας μέσω των Apple Smartphone, iPad και λάπτοπ τους.

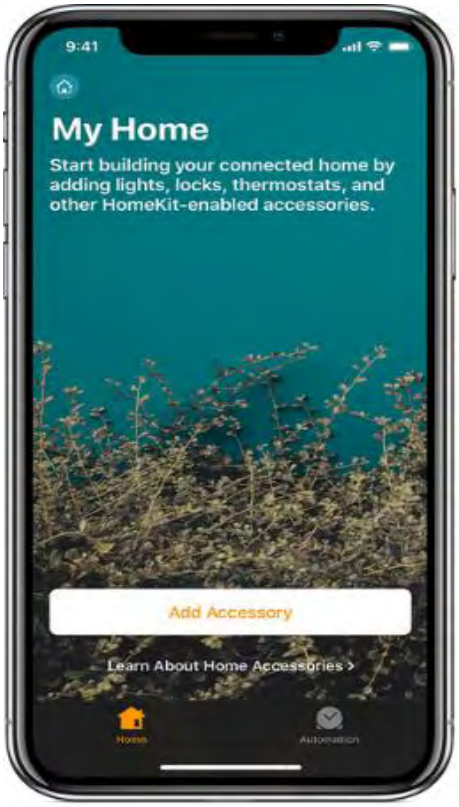
3D κάτοψη της οικίας

Σύμφωνα με τον προϋπολογισμό της οικογένειας, ο μηχανικός που ανέλαβε την εξυπηρέτηση της, πρότεινε έξυπνες συσκευές οι οποίες είναι συμβατές με το Apple HomeKit ή με το Apple AirPlay και μπορούν να ελεγχθούν μέσω της εφαρμογής Home App. Επίσης είναι δυνατή η εγκατάσταση οικιακών αυτοματισμών που είναι εξίσου διαχειρίσιμες μέσω του Home app. Η συμβατότητα με το HomeKit σημαίνει ότι οι ιδιοκτήτες μπορούν να πουν: "Siri, turn the light off", και αυτό να γίνει, δηλαδή να σβήσουν τα φώτα. Η τεχνολογία του Apple HomeKit παρέχει προηγμένη ασφάλεια, με απ' άκρη σ' άκρη κρυπτογράφηση και αυθεντικοποίηση μεταξύ των HomeKit-enabled συσκευών και του iPhone, iPad, ή iPod touch μας.

Για το Home app, αυτό που χρειάζεται είναι οι ιδιοκτήτες να αναβαθμίσουν τα iPhone, iPad και iPod touch στην τελευταία έκδοση του iOS. Για χρήση του Home app σε Mac, πρέπει να γίνει αναβάθμιση του Mac σε macOS Mojave. Για τον έλεγχο του σπιτιού μέσω του Home app, απαιτείται επίσης sign in στο iCloud χρησιμοποιώντας την Apple ID σε κάθε συσκευή. Στη συνέχεια χρειάζεται ενεργοποίηση των iCloud Keychain και Home στις ρυθμίσεις του iCloud.

Στο μέλλον, η οικογένεια πρόκειται να αγοράσει κι άλλες έξυπνες συσκευές οι οποίες θα πρέπει επίσης να είναι συμβατές με τις παρακάτω εφαρμογές. Για να προσθέσει μια επιπλέον συσκευή (accessory) στο Home app, πρέπει να χρησιμοποιήσει μια από τις συσκευές με iOS, καθώς δεν μπορεί να γίνει αυτό χρησιμοποιώντας Mac. Περισσότερες πληροφορίες υπάρχουν στην ιστοσελίδα της Apple και συγκεκριμένα εδώ: [214-218]

Τα σύμβολα των ομώνυμων εφαρμογών [163]



Το γραφικό περιβάλλον του Home app σε iPhone X [216]

Οι έξυπνες συσκευές που προτάθηκαν, είναι συμβατές με το Apple HomeKit ή με το Apple AirPlay και πολλές από αυτές έχουν ενσωματωμένη και την Amazon Alexa, και είναι οι εξής [223]:

Cisco RV132W ADSL2+-> 90€
Linksys WAP300N Wireless Access Point N300 Dual-Band->50€
Schlage Sense Smart Deadbolt->165€
ecobee3 2 x Room Sensors 2 pack->142€
iHome ISP6X Smart Plug-> 3*22 = 66€
Sylvania 74579 SMART+ A19 Soft White LED Bulb->6*18 = 108€
D-Link Omna 180 Cam HD Camera->115€
Sylvania Smart+ In Wall Switch-> 33€
iHome ISP100-> 30€
Lifx Mini-> 8*13 = 104€
ecobee Switch+->65€
Lutron Serena smart Shades and lights, The Caséta Wireless Smart Lighting Lamp Dimmer Kit, Homekit-enabled->167€
Koogeek Wi-Fi Enabled Smart Socket E27 Light Bulb Adapter Monitor Power->2*35E=70€
Mr. Coffee® Simple Brew 12-Cup Programmable Coffee Maker Black->27€
Marantz SR5013 7.2 Channel AV Receiver->880€
Apple HomePod-> 300€
Elgato Eve Motion Sensor->35€
Lightwave Link Plus (bridge)->115€

ecobee3 lite Smart Thermostat ->150€
OEM U/UTP Cat.5e Cable 10m Γκρί ->2,19€
Παροχή πλήρους σχεδιασμού και υλοποίησης του έξυπνου οικιακού δικτύου, μετέπειτα συντήρησης και τεχνικής υποστήριξης -> 1000€
Μερικό Σύνολο: 3.714,19€

Οι παρακάτω εικόνες αφορούν τις συσκευές που προτείνονται για χρήση στους ιδιοκτήτες του έξυπνου σπιτιού αυτής της μελέτης.

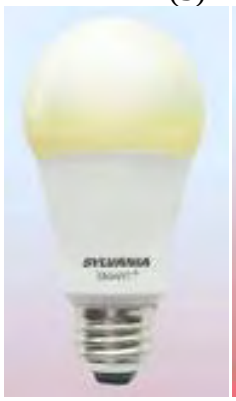
(1)

(2)

(3)

(4)

(5)



(6)

(7)

(8)

(9)

(10)

(11)

(12)

(13)

(14)

(15)

(16)

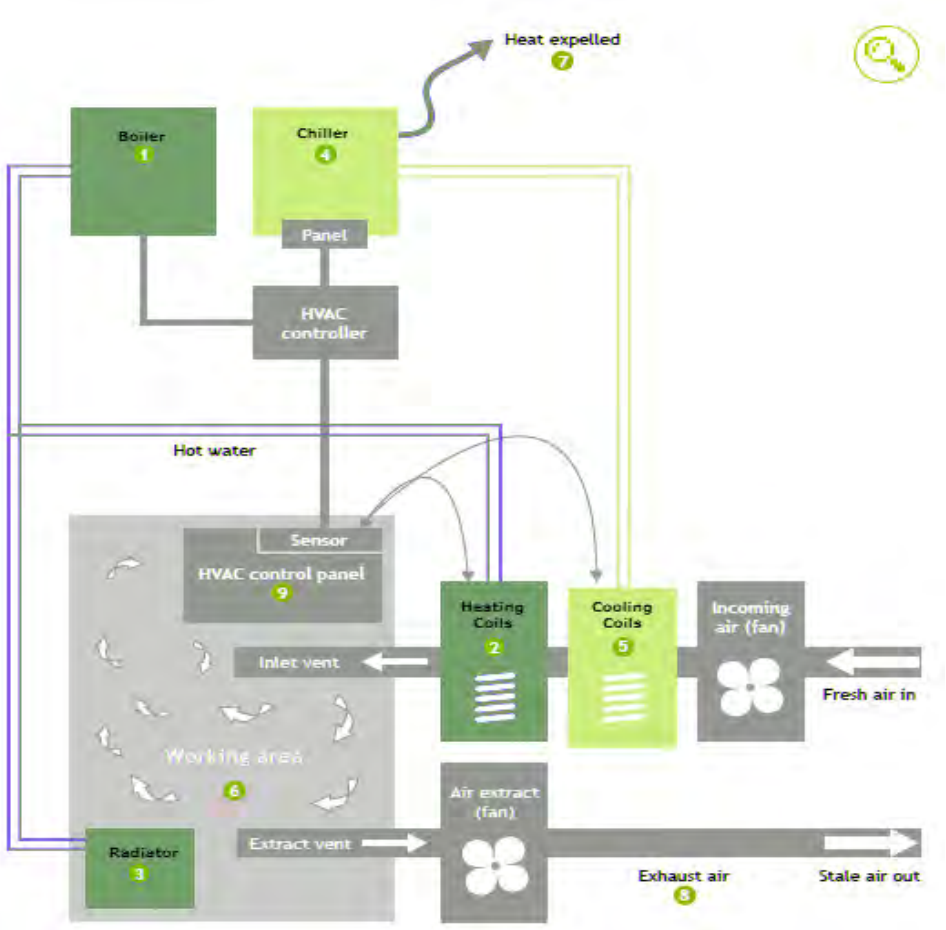
(17)

(18)

(19)

Το Lightwave Link Plus [172] βρίσκεται στην καρδιά του έξυπνου σπιτιού προσφέροντας ασφαλή, εύκολο και απομακρυσμένο έλεγχο και χειρισμό των έξυπνων οικιακών συσκευών. Ξεπερνά σε ισχύ τα περισσότερα Wi-Fi ρούτερς καλύπτοντας με άνεση έως και 3 ορόφους. Είναι συμβατό με Apple HomeKit, Amazon Alexa, Google Assistant και IFTTT.

Συγκεκριμένα, για τη θέρμανση, τον εξαερισμό και τον κλιματισμό (HVAC), επιλέχθηκε το ecobee3 lite Smart Thermostat που θα συνδεθεί στο υπάρχον δίκτυο HVAC του σπιτιού και 6 αισθητήρες θερμοκρασίας και υγρασίας που θα κατανεμηθούν στους έξι χώρους του σπιτιού. Τα συστήματα HVAC συνιστώνται ως επί το πλείστον από τα δομικά στοιχεία που φαίνονται στην παρακάτω εικόνα.

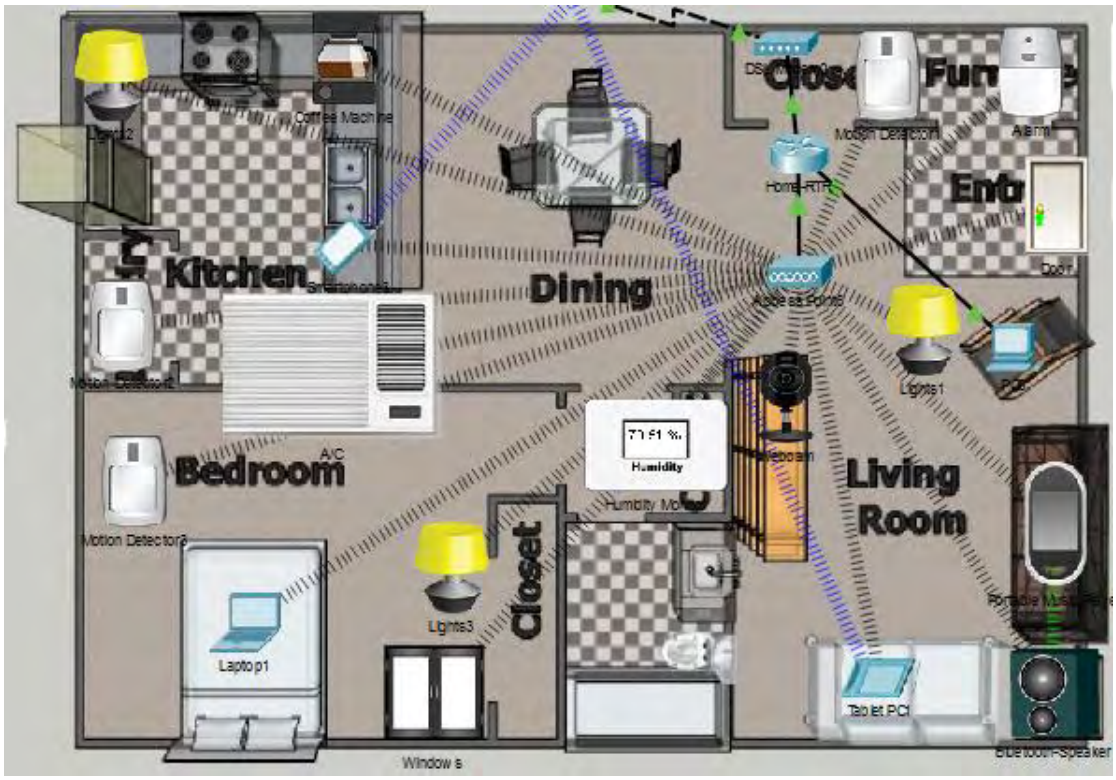


HVAC components [170]

Το (19) ecobee3 lite που έρχεται μαζί με δύο αισθητήρες θερμοκρασίας [173], αποτελεί το HVAC control panel και συντονίζει όλα τα επιμέρους στοιχεία του HVAC ώστε να λειτουργούν αρμονικά μεταξύ τους. Η κεντρική μονάδα ελέγχου σβήνει, ανάβει, ελέγχει και προσαρμόζει chillers, boilers, θερμοκρασίες, πιέσεις και νερό ανάλογα με τον τρόπο που έχει ρυθμιστεί και με τα δεδομένα που λαμβάνει από τους αισθητήρες κάθε χώρου. Φυσικά, οι απαιτήσεις θερμοκρασίας κάθε χώρου είναι διαφορετικές. Για παράδειγμα, η ιδανική θερμοκρασία για το χώρο του μπάνιου είναι 23 βαθμοί Celsius, ενώ το υπνοδωμάτιο μπορεί να είναι πιο δροσερό, από 15 έως 20 βαθμούς. [171]

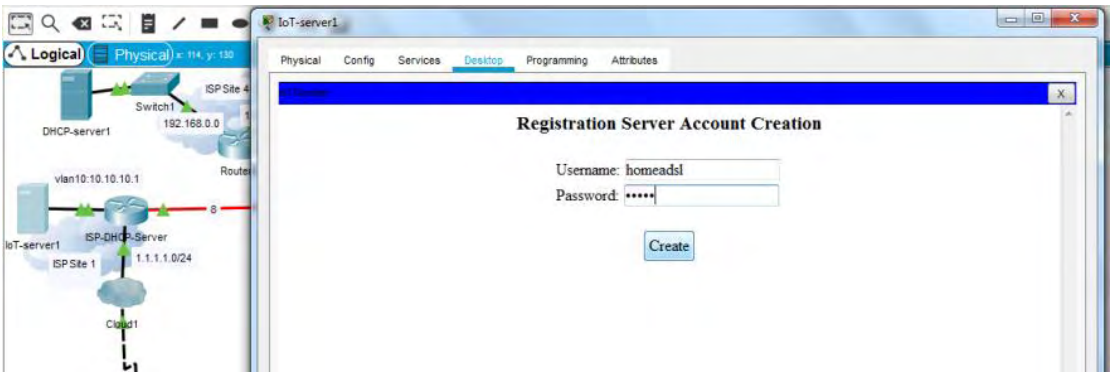
5.2 Σχεδιασμός σχήματος Διευθυνσιοδότηση *Συσκευών*

5.2.1 Σημεία πρόσβασης IPv4



Το έξυπνο σπίτι του σεναρίου

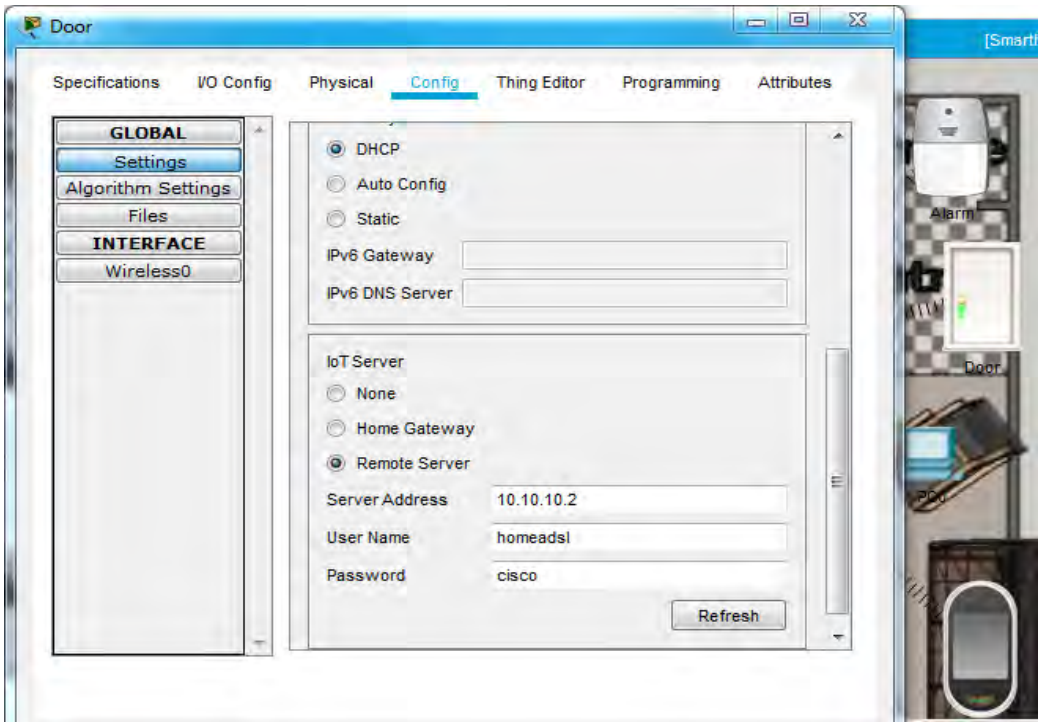
Ο IoT εξυπηρετητής (IoT registration server) για την έξυπνη οικία του σεναρίου μας είναι μια υπηρεσία που προσφέρεται από τον ISP. Στα πλαίσια της προσομοίωσης, ρυθμίστηκε ώστε να προσφέρει IoT υπηρεσίες για τις IoT συσκευές του σπιτιού, ώστε να μπορούμε να τις χειριστούμε απομακρυσμένα (και όταν είμαστε εκτός σπιτιού), κάτι που δεν θα μπορούσαμε να κάνουμε αν είχαμε χρησιμοποιήσει μια home gateway.



Δημιουργία λογαριασμού στον IoT server

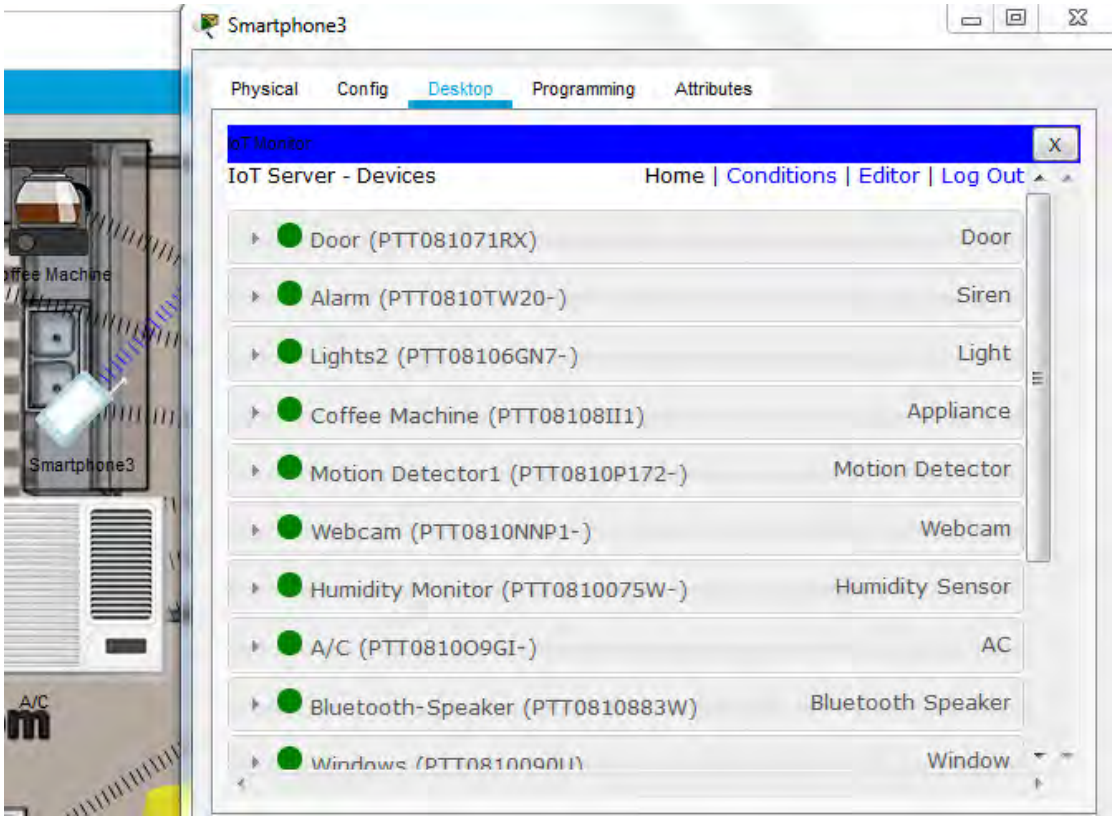
Είναι πολύ σημαντικό πρώτα να εγκαταστήσουμε τον server και μετά να συνδεθούμε με το παραπάνω όνομα και κωδικό, πριν ακόμη κάνουμε εγγραφή όλων των IoT συσκευών στον IoT

server. Στο επόμενο βήμα γίνεται η εγγραφή των IoT συσκευών της οικίας καταχωρώντας τα στοιχεία του remote server, με όνομα χρήστη: homeadsl και κωδικό: cisco, όπως φαίνεται στην παρακάτω εικόνα.

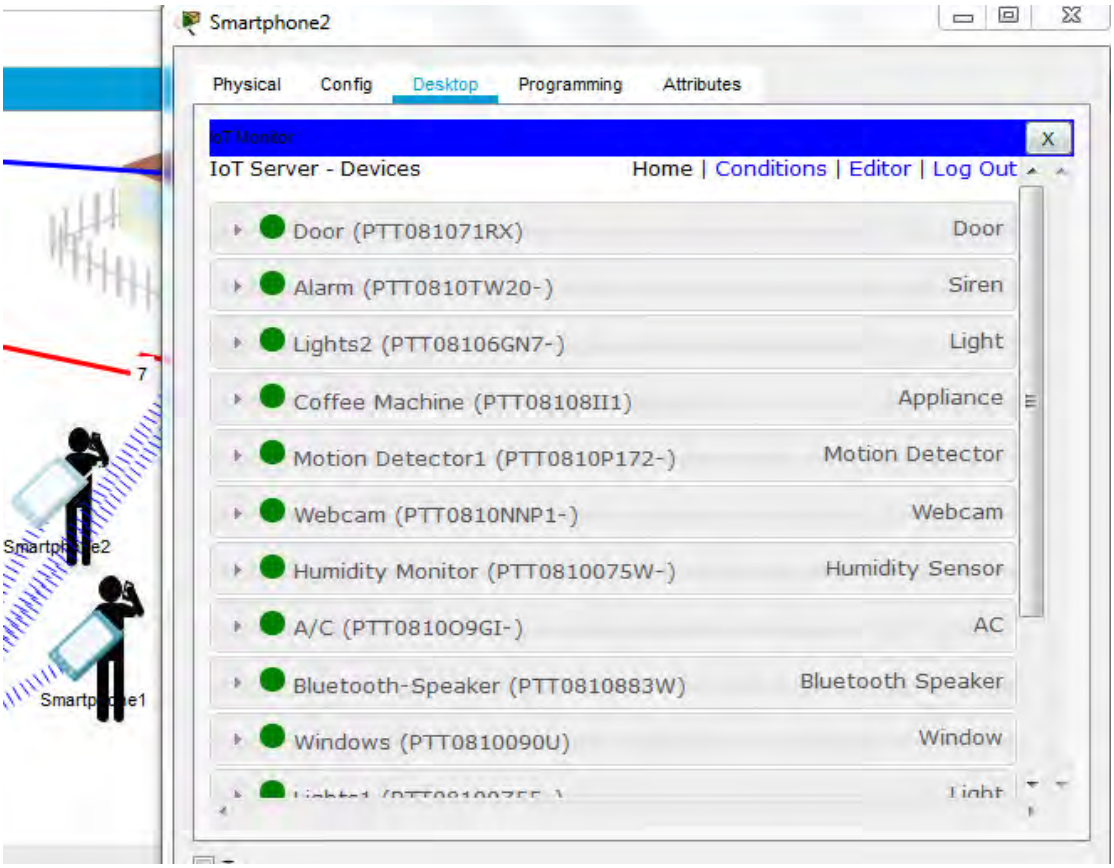


Εγγραφή της έξυπνης πόρτας στον IoT server

Στις παρακάτω εικόνες, φαίνεται η παρακολούθηση των IoT συσκευών από το smartphone που βρίσκεται εντός του σπιτιού και από το smartphone ενός μέλους της οικογένειας που βρίσκεται εκτός του σπιτιού. Όπως παρατηρούμε, και στις δύο περιπτώσεις έχουμε ακριβώς τις ίδιες δυνατότητες ελέγχου και διαχείρισης του έξυπνου οικιακού μας δικτύου.

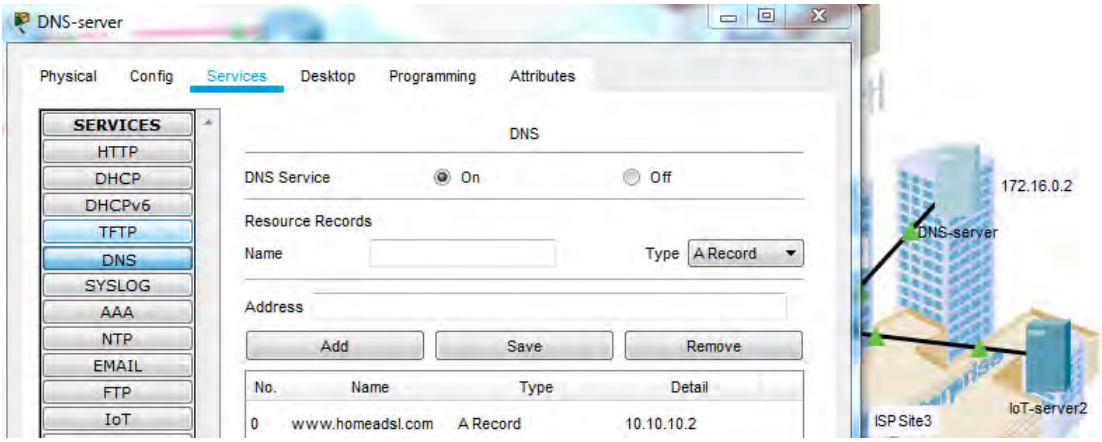


Έλεγχος των IoT συσκευών μέσω Smartphone εντός του σπιτιού



Απομακρυσμένος έλεγχος των IoT συσκευών μέσω Smartphone εκτός του σπιτιού

Η πρόσβαση επίσης στο οικιακό δίκτυο μπορεί να επιτευχθεί μέσω της υπηρεσίας Ίντερνετ που μας προσφέρει επίσης ο ISP. Στην προσομοίωση, ρυθμίσαμε έναν εξυπηρετητή του ISP ώστε να είναι ο DNS server.



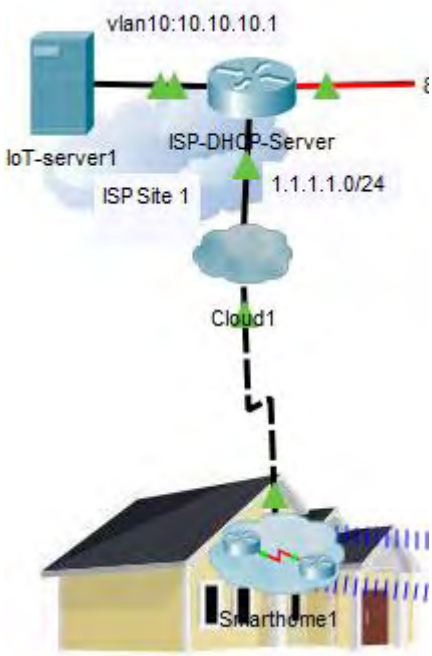
Ρύθμιση του DNS server του ISP

Για την πιο εύκολη διαχείριση των ρυθμίσεων TCP/IP, προτάθηκε η χρήση του αυτόματου πρωτοκόλλου δυναμικής ρύθμισης παραμέτρων κεντρικών υπολογιστών (DHCP). Το DHCP εκχωρεί αυτόματα διευθύνσεις πρωτοκόλλων Internet (IP) στους υπολογιστές του δικτύου, εάν το δίκτυο το υποστηρίζει. Εφόσον χρησιμοποιήσουμε το πρωτόκολλο DHCP, τότε δεν χρειάζεται οι ένοικοι του σπιτιού να αλλάζουν τις ρυθμίσεις TCP/IP, όταν μετακινούν τον υπολογιστή τους σε άλλη θέση, ή κυρίως όταν προσθέτουν κι άλλες IoT συσκευές. Οι νέες IoT συσκευές (clients) θα λαμβάνουν αυτόματα τις ρυθμίσεις παραμέτρων του δικτύου με το που συνδεθούν στο οικιακό δίκτυο. Σε τέτοια δίκτυα, οι χειροκίνητες ρυθμίσεις θα απαιτούσαν πολύ χρόνο. Με την αυτόματη δέσμευση ενός υπολογιστή στο δίκτυο μέσω του DHCP, ο χρήστης γλιτώνει από την εκτέλεση των συγκεκριμένων εργασιών. Αρκεί ένας διαχειριστής να διαμορφώσει μια φορά τις απαραίτητες ρυθμίσεις παραμετροποίησης όπως κάναμε κι εμείς στον οικιακό router.

```
ip dhcp excluded-address 192.168.11.1
ip dhcp excluded-address 192.168.11.2
!
ip dhcp pool Home_Users
 network 192.168.11.0 255.255.255.0
 default-router 192.168.11.1
 dns-server 172.16.0.2
```

DHCP ρυθμίσεις στον οικιακό router

Όλες οι ασύρματες συσκευές πρέπει να χρησιμοποιούν το ίδιο SSID, password και DHCP προεπιλεγμένες ρυθμίσεις, εκτός των διακομιστών στους οποίους πρέπει πάντα να χρησιμοποιείται static IP. Οι στατικές IPs διασφαλίζουν ότι ακόμη και με επανεκκίνηση του WLAN router ή του Access Point, η IP του server θα παραμείνει η ίδια και δεν θα χρειάζεται να ξανά ρυθμιστούν οι IoT συσκευές με τη νέα IP του IoT server.



Οι ISP DHCP και IoT servers για το παρόν smarthome

Ο παρακάτω πίνακας παρουσιάζει την διευθυνσιοδότηση όλων των συσκευών της προσομοίωσης.

Πίνακας Διευθύνσεων IPv4

Device	Interface	IPv4 address/subnet mask	Default Gateway	DNS server
Router0	F0/0	172.16.0.1/16	N/A	N/A
	S0/1/0	192.168.100.26/30	N/A	N/A
Router1	F0/0	172.19.0.1/16	N/A	N/A
	S0/3/0	192.168.100.34/30	N/A	N/A
Router2	Fa1/0	192.168.100.1/30	N/A	N/A
	S0/3/0	192.168.100.5/30	N/A	N/A
	S0/3/1	192.168.100.9/30	N/A	N/A
Router3	F1/0	192.168.100.29/30	N/A	N/A
	S0/1/0	192.168.100.17/30	N/A	N/A
	S0/3/0	192.168.100.6/30	N/A	N/A
	S0/3/1	192.168.100.13/30	N/A	N/A
ISP-DHCP-Server	F0/0	1.1.1.1.0/24	N/A	172.16.0.2
	F/0/2/0-3 (Vlan 10)	10.10.10.0/24	10.10.10.0/24	N/A
	F1/0	192.168.100.30/30	N/A	N/A
Router6	S0/1/0	192.168.100.18/30	N/A	N/A
	S0/1/1	192.168.100.21/30	N/A	N/A
	S0/2/0	192.168.100.33/30	N/A	N/A
Router7	S0/1/0	192.168.100.22/30	N/A	N/A
	S0/1/1	192.168.100.10/30	N/A	N/A

	S0/2/0	192.168.100.14/30	N/A	N/A
	S0/2/1	192.168.100.25/30	N/A	N/A
Router8	F0/0	192.168.10.1/30	N/A	N/A
	F0/1	192.168.0.1/30	N/A	N/A
	F1/0	192.168.100.2/30	N/A	N/A
DHCP-server1 (testing for smarthome2)	F0	192.168.0.2/24	192.168.0.1	N/A
CO-server0	backbone	172.19.0.2/16	172.19.0.1	N/A
	cellular	172.16.1.1/24	N/A	N/A
DNS-server	F0	172.16.0.2/16	172.16.0.1	N/A
IoT-server1	F0	10.10.10.2	10.10.10.1	172.16.0.2
IoT-server2 (testing for smarthome2)	F0	172.16.0.3/16	172.16.0.1	172.16.0.2
Smartphone1	wireless	N/A	N/A	DHCP
	3G/4G Cell1	DHCP	DHCP	
Smartphone2	wireless	N/A	N/A	DHCP
	3G/4G Cell1	DHCP	DHCP	

Πίνακας Διευθύνσεων IPv4 του Smarthome1

Device	Interface	IPv4 address/subnet mask	Default Gateway	DNS server	IoT Remote Server
Smartphone 3	Wireless1	DHCP	DHCP	DHCP	N/A
	3G/4G Cell1	DHCP	DHCP	DHCP	N/A
Laptop1	Wirelless1	DHCP	DHCP	DHCP	N/A
Tablet PC1	Wireless1	DHCP	DHCP	DHCP	N/A
	3G/4G Cell1	DHCP	DHCP	DHCP	N/A
Door	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Window	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Bluetooth Speaker	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Webcam	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Coffee Appliance	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
AC	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Lights1	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Lights2	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Lights3	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Motion Detector1	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Motion Detector2	Wireless1	DHCP	DHCP	DHCP	10.10.10.2

Motion Detector3	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Humidity Monitor	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Furnace	Wireless1	DHCP	DHCP	DHCP	10.10.10.2
Portable Music Player	Wireless1	DHCP	DHCP	DHCP	N/A

Πίνακας Διευθύνσεων IPv4 του testing Smarthome2

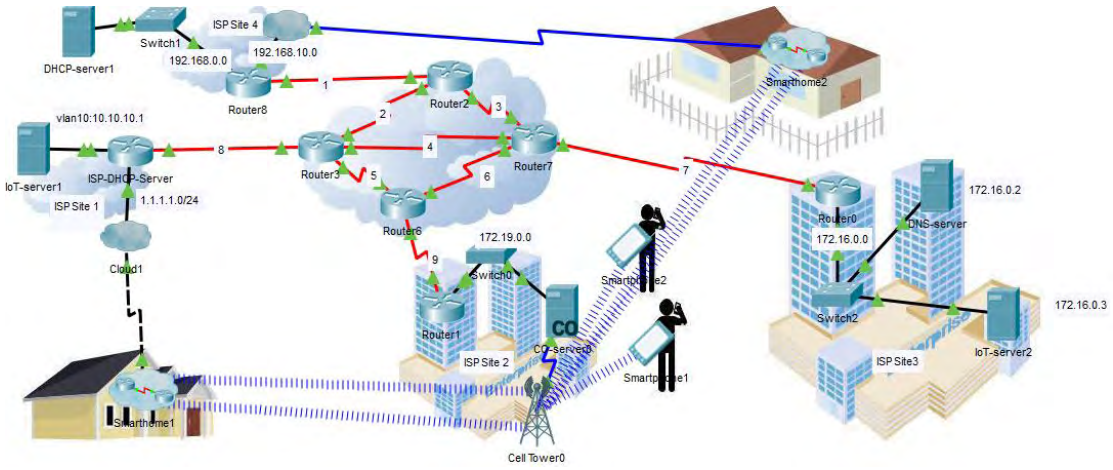
Device	Interface	IPv4 address/subnet mask	Default Gateway	DNS server	IoT Remote Server
Smartphone0	Wireless0	DHCP	DHCP	DHCP	N/A
	3G/4G Cell1	DHCP	DHCP	DHCP	N/A
Laptop0	Wireless0	DHCP	DHCP	DHCP	N/A
Tablet PC0	Wireless0	DHCP	DHCP	DHCP	N/A
Door	Wireless0	DHCP	DHCP	DHCP	172.16.0.3
Window	Wireless0	DHCP	DHCP	DHCP	172.16.0.3
AC	Wireless0	DHCP	DHCP	DHCP	172.16.0.3
Light	Wireless0	DHCP	DHCP	DHCP	172.16.0.3
Webcam	Wireless0	DHCP	DHCP	DHCP	172.16.0.3
Coffee Appliance	Wireless0	DHCP	DHCP	DHCP	172.16.0.3
TV	Wireless0	DHCP	DHCP	DHCP	172.16.0.3
Ceiling Fan	Wireless0	DHCP	DHCP	DHCP	172.16.0.3

5.3 Τοπολογία και Συνδεσιμότητα

Ας υποθέσουμε το παρακάτω σενάριο. Σχεδιασμός του δικτύου μιας έξυπνης κατοικίας μιας ευρωπαϊκής πόλης όπου οι ένοικοι του θα μπορούν να διαχειριστούν ακόμη και απομακρυσμένα τις έξυπνες συσκευές τους. Στις παρακάτω εικόνες φαίνεται η ευρωπαϊκή πόλη του σεναρίου μας καθώς ςκαι η λογική τοπολογία του δικτύου του σεναρίου.

Νυχτερινή φωτογραφία της ευρωπαϊκής πρωτεύουσας από δορυφόρο, Packet Tracer Physical View

Νυχτερινή φωτογραφία της πόλης του σεναρίου, Packet Tracer Physical View



Η τοπολογία του δικτύου της πόλης, Packet Tracer Logical View

Η προσομοίωση του δικτύου της πόλης που σχεδιάζουμε αποτελείται από 7 τμήματα:

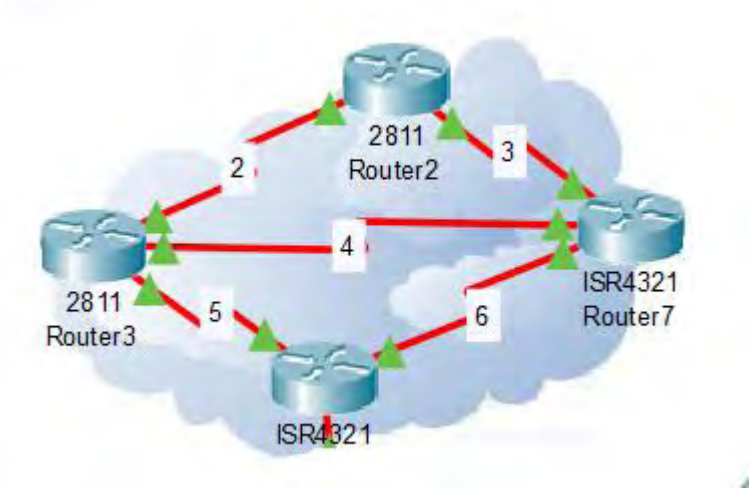
- Smarthome1
- Smarthome2 (testing)
- Cloud1 (ISP site 1 όπου ανήκει ο IoT-server1 και ο ISP-DHCP-Server)
- Cloud0 (ISP site 4 όπου ανήκει ο DHCP-server για το Testing Smarthome2)
- Enterprise1 (ISP site 2 όπου ανήκει ο το Cell Tower)
- Enterprise2 (ISP site 1 όπου ανήκουν ο DNS server και ο IoT-server2)
- 4 Core routers

Συνολικά, χρειάστηκαν 8 core routers για να προσομοιώσουν την ύπαρξη ολοκληρωμένων ανεξάρτητων διασυνδεδεμένων δικτύων για τις ανάγκες της εργασίας. Θα γίνει αναφορά σε ολόκληρη την σχεδίαση και την παραμετροποίση των συσκευών της τοπολογίας αλλά η τεχνοοικονομική μελέτη αφορά τα Smarthome 1 και Smarthome 2. Συγκεκριμένα στην τοπολογία έχουμε τοποθετήσει:

- 8 Core routers
- DHCP servers
- 1 DNS server
- IoT servers
- 1 Central-Office server
- 1 Cell tower

Όσον αφορά στη συνδεσιμότητα, η δομημένη καλωδίωση (Structured Cabling) είναι αυτή που ασχολείται κυρίως με τον τρόπο που θα εγκατασταθούν τα μέσα μετάδοσης που θα χρειαστούν για να συνδεθούν δικτυακές συσκευές σε κτίρια. Η δομημένη καλωδίωση αφορά τη δομή της καλωδιακής εγκατάστασης ενός τοπικού δικτύου και τις προδιαγραφές που αυτή θα πρέπει να διαθέτει. Αποτελεί σημαντικό παράγοντα για τις μελλοντικές φυσικές επεκτάσεις του δικτύου, για τις αναδιατάξεις των δομικών στοιχείων του, καθώς και για την αναβάθμιση των

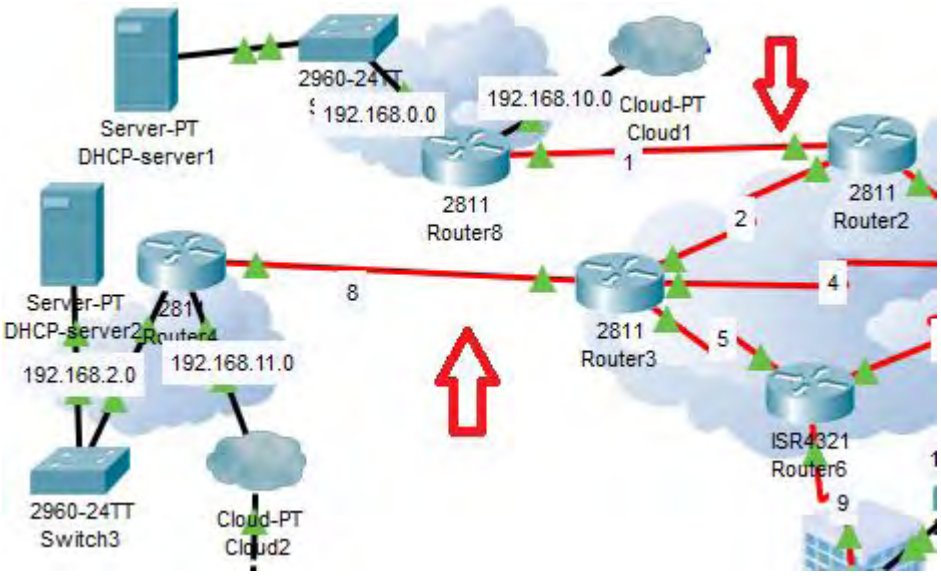
προσφερόμενων υπηρεσιών του [175]. Η δομημένη καλωδίωση ανήκει στο OSI Layer 1. Χωρίς Layer 1 συνδεσιμότητα, δεν είναι εφικτές οι Layer2 και Layer 3 switching και routing διαδικασίες αντίστοιχα, καθιστώντας αδύνατη τη μεταφορά δεδομένων μεταξύ των δικτύων.
Στη δική μας τοπολογία, για τους 4 κεντρικούς routers χρησιμοποιήσαμε serial καλωδίωση που χρησιμοποιείται για T1, E1, T3 κ.ά. τύπους WAN συνδεσιμότητας για μεγάλες αποστάσεις συνήθως με έναν Service Provider, όπως φαίνεται στην παρακάτω εικόνα. Για παράδειγμα, εάν έχεις 2 sites, το ένα στο Los Angeles και το άλλο στο San Francisco και θες να χρησιμοποιήσεις T1 για να συνδέσεις αυτά τα δύο sites, χρησιμοποιείς μια T1/Serial card σε καθέναν από τους δυο routers σου σε αυτές τις περιοχές και χρησιμοποιείς Service Providers όπως η Verizon και η AT&T για να συνδέσεις αυτά τα sites.



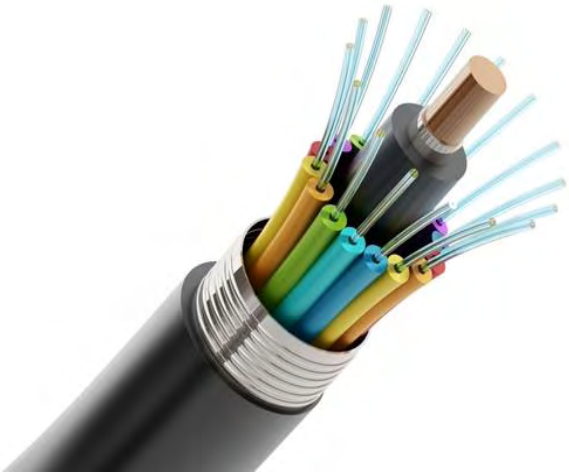
Serial καλωδίωση μεταξύ των router

Serial Cisco router cable [180]

Στη συνέχεια, για να συνδέσουμε τον router 2 με τον router 8 και τον router 3 με τον router 4, χρησιμοποιήσαμε καλώδια οπτικών ινών (fiber), όπως φαίνεται στην παρακάτω εικόνα. Αυτό έγινε γιατί η καλωδίωση UTP για Ethernet έχει περιορισμό για την οριζόντια (ή fixed) συνιστώμενη απόσταση τα 90 μέτρα ώστε να αποφεύγεται η εξασθένιση του σήματος. Οι οπτικές ίνες αντίστοιχα μπορούν να προσφέρουν κάλυψη μεγαλύτερης απόστασης, 500 μέτρα έως και μερικά χιλιόμετρα, εξαρτάται από την τεχνολογία. [174]. Ένας ακόμη λόγος που σε αυτούς τους routers επιλέξαμε να τοποθετήσουμε οπτικές ίνες είναι ότι και στα δυο αυτά sites υπάρχει από ένας server ο οποίος έχει περισσότερες ανάγκες για bandwidth.

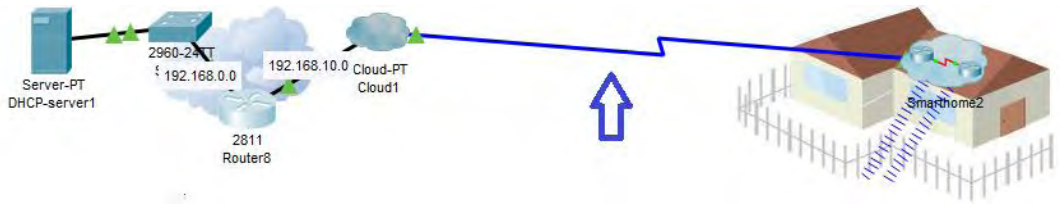


Fiber καλωδίωση μεταξύ των router στην προσομοίωση



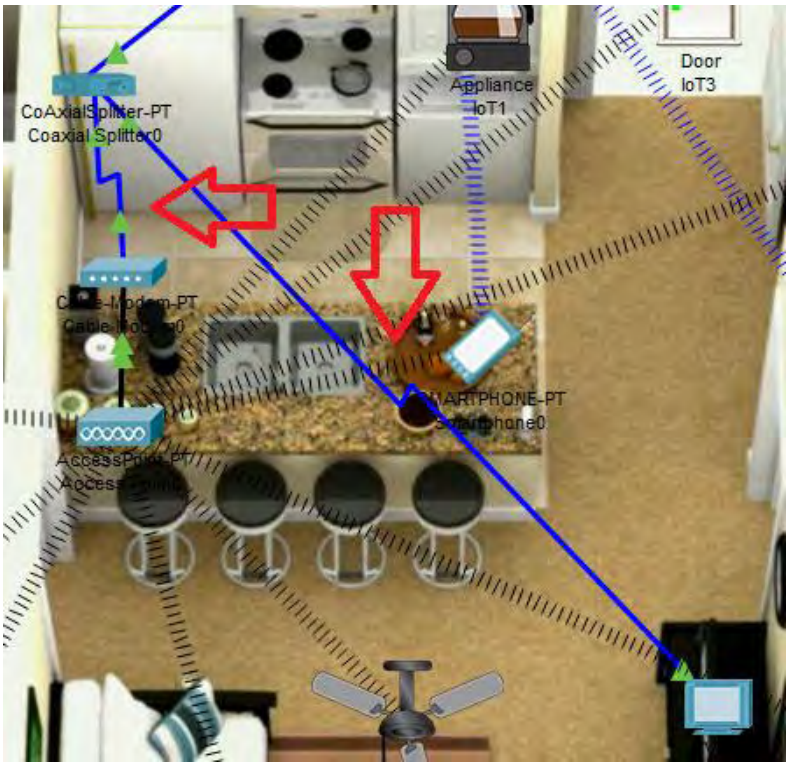
Multi-fiber cable [179]

Επίσης, χρησιμοποιήσαμε ομοαξονικό καλώδιο (coaxial cabling) στις παρακάτω 3 περιπτώσεις, όπως φαίνεται στις εικόνες. Το ομοαξονικό καλώδιο είναι η γραμμή μεταφοράς του ηλεκτρομαγνητικού σήματος δηλαδή ο συνδετικός κρίκος μεταξύ του κεραιοσυστήματος και του δορυφορικού μας δέκτη.

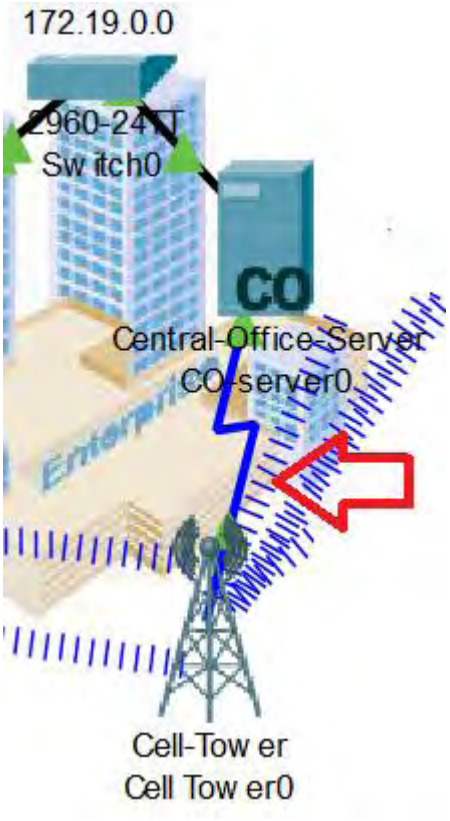


Χρήση ομοαξονικού καλωδίου (1)

Το ομοαξονικό καλώδιο που χρησιμοποιείται στην δορυφορική λήψη, χρησιμοποιείται και στην πλειοψηφία των επιγείων εγκαταστάσεων για την διανομή του σήματος στα διάφορα σημεία μιας κατοικίας.

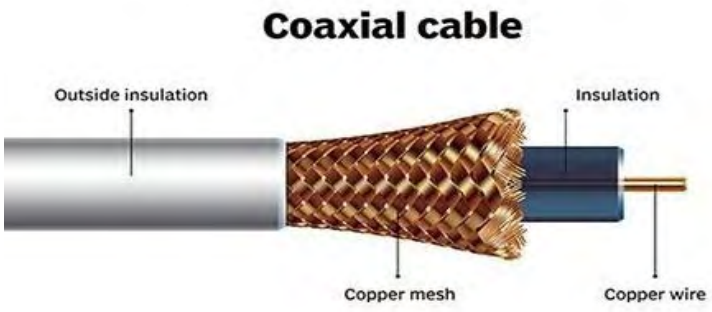


Χρήση ομοαξονικού καλωδίου στο testing smarthome2 (2)



Χρήση ομοαξονικού καλωδίου (3)

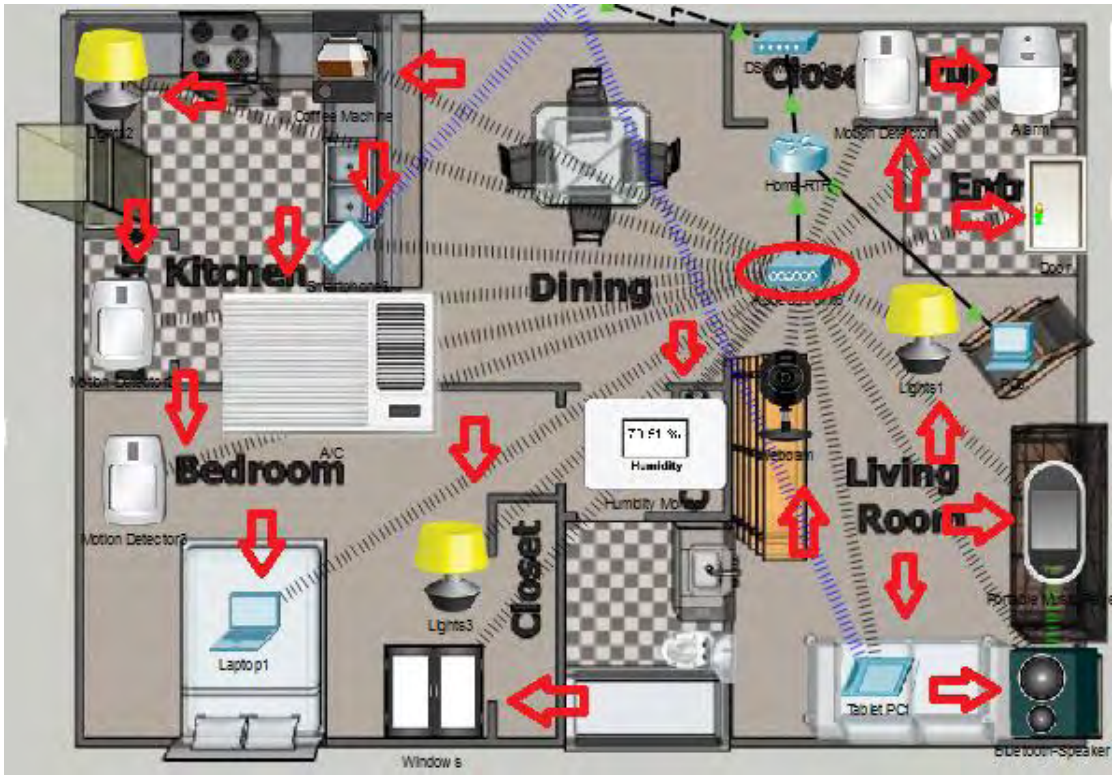
Το ομοαξονικό καλώδιο διαφέρει από τα άλλα θωρακισμένα καλώδια επειδή οι διαστάσεις του ελέγχονται για να δώσουν ένα ακριβές, σταθερό διάστημα αγωγών που απαιτείται για να λειτουργήσει αποτελεσματικά ως γραμμή μεταφοράς. Χρησιμοποιείται για την διέλευση ηλεκτρικών σημάτων μεγάλου εύρους συχνοτήτων. Για παράδειγμα μπορεί να μεταφέρει ηχητικά σήματα από ένα ακουστικό ενισχυτή μέχρι και ηλεκτρικά σήματα πολλών Mega Hertz. [176]



Ομοαξονικό καλώδιο [178]

Δεν είναι όλα τα μέσα μετάδοσης φυσικά, όπως συμβαίνει στην περίπτωση των ασύρματων τεχνολογιών. Οι ασύρματοι χρήστες/συσκευές των smarthomes της τοπολογίας μας αποκτούν πρόσβαση στο ενσύρματο δίκτυο επικοινωνώντας μέσω ραδιοκυμάτων με ένα ασύρματο Access Point (AP). Το AP με τη σειρά του είναι άμεσα καλωδιωμένο με το οικιακό LAN. Όλες οι ασύρματα συνδεδεμένες συσκευές με το ίδιο AP μοιράζονται το ίδιο τμήμα του

δικτύου που σημαίνει ότι μόνο μια συσκευή μπορεί να στείλει και να λάβει δεδομένα από το AP την κάθε χρονική στιγμή (half duplex communication).

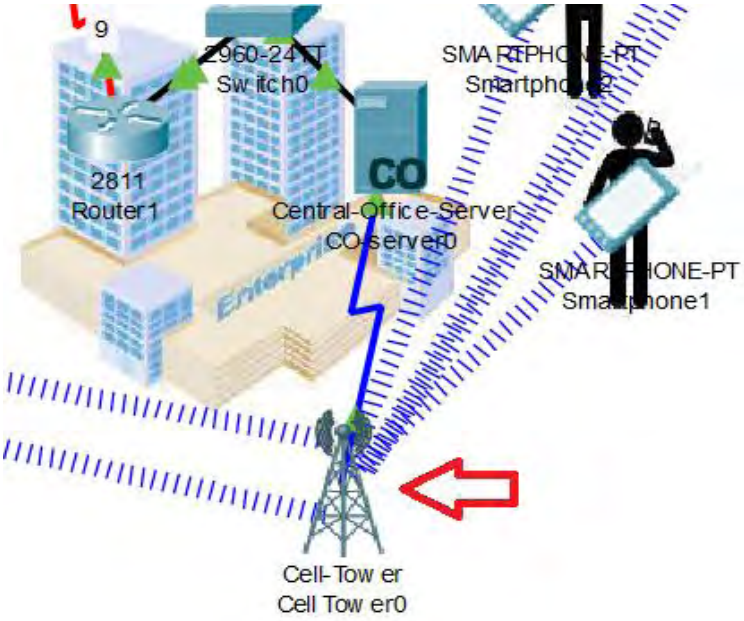


Το AP και οι ασύρματα συνδεδεμένες σε αυτό συσκευές

Επίσης στην τοπολογία του δικτύου χρησιμοποιήθηκε ένας πύργος κινητής τηλεφωνίας (Cell Tower) για να προσομοιώσει την ύπαρξη ενός ασύρματου δικτύου κινητής τηλεφωνίας για τη χρήση κινητών τηλεφώνων. Όταν χρησιμοποιούμε το κινητό μας τηλέφωνο για να επικοινωνήσουμε, τότε αυτό στέλνει και λαμβάνει ηλεκτρομαγνητικά σήματα προς και από έναν σταθμό βάσης, ο οποίος στη συνέχεια επικοινωνεί ενσύρματα ή ασύρματα με κάποια κέντρα αναδιανέμοντας την πληροφορία, ώστε να μπορούμε να επικοινωνούμε με αυτούς που θέλουμε.

Συγκεκριμένα, οι σταθερές κεραίες που χρησιμοποιούνται για την εξυπηρέτηση της κινητής τηλεφωνίας αναφέρονται ως σταθμοί βάσης κυψελωτών επικοινωνιών ή πύργοι μετάδοσης κινητής τηλεφωνίας. Οι σταθμοί βάσης αποτελούνται από τις κεραίες και τον ηλεκτρονικό εξοπλισμό. Τα σήματα τροφοδοτούνται προς τις κεραίες μέσω καλωδίων και στη συνέχεια, εκπέμπονται ως ραδιοκύματα στην περιοχή που περιβάλλει το σταθμό βάσης. Στους σταθμούς βάσης υπάρχουν και κεραίες σε σχήμα πιάτου/τυμπάνου (dish antenna), οι οποίες αποτελούν τερματικούς κόμβους για τη μικροκυματική σύνδεση και επικοινωνία με άλλους σταθμούς βάσης, εξυπηρετούν δηλαδή τη διασύνδεση του δικτύου. Μερικές φορές, οι σταθμοί βάσης διασυνδέονται μεταξύ τους με υπόγεια καλώδια αντί με μικροκυματικές ασύρματες ζεύξεις.

Ανάλογα με τη θέση του σταθμού βάσης και το πλήθος των εξυπηρετουμένων χρηστών κινητών τηλεφώνων, οι σταθμοί βάσης μπορεί να απέχουν μεταξύ τους από μερικές εκατοντάδες μέτρα σε μεγάλες πόλεις έως αρκετά χιλιόμετρα σε αγροτικές περιοχές. [177]



Πύργος κινητής τηλεφωνίας της προσομοίωσης

Πύργος κινητής τηλεφωνίας [177]

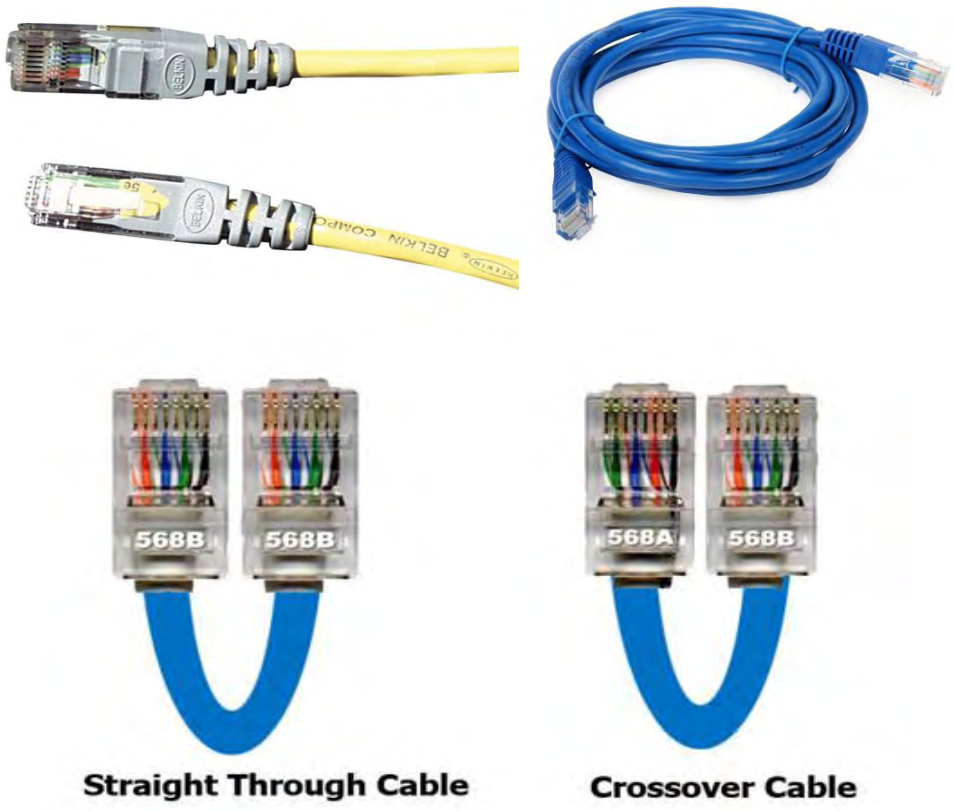
Τις περισσότερες φορές στην τοπολογία μας, τόσο στην πόλη όσο και στα smarthomes, χρησιμοποιήσαμε καλώδιο Ethernet. Το Ethernet είναι το συνηθέστερα χρησιμοποιούμενο πρότυπο δίκτυο υπολογιστών ενσύρματης τοπικής δικτύωσης υπολογιστών. Οι νεότερες εκδόσεις του Ethernet οι οποίες χρησιμοποιούν είτε κοινά αθωράκιστα καλώδια χαλκού (καλώδια UTP) ή θωρακισμένα συνεστραμμένα ζεύγη αγωγών (καλώδια STP) ή οπτικές ίνες είναι: Ethernet (10Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), 10 Gigabit Ethernet (10Gbps). Τα καλώδια Ethernet συνδέουν τις συσκευές δικτύου όπως modem, routers και κάρτες δικτύου. Μεταδίδουν δεδομένα με την χρήση του πρωτοκόλλου Ethernet. Τα καλώδια Ethernet χρησιμοποιούν συνδέσεις RJ-45 και στα δύο άκρα. Η κάθε μια άκρη έχει 8pin. Τα περισσότερα καλώδια είναι κατηγορίας CAT-5 (ή και 5e) το οποίο σημαίνει ότι υποστηρίζουν ταχύτητα 100MB/sec. Ονομάζονται και 10/100 Base-T Cat 5 [181]. Κάποια καλώδια είναι straight through και κάποια άλλα crossover. Τα straight through είναι καλώδια που το πρώτο

σύρμα είναι συνδεδεμένο με το πρώτο σύρμα της άλλης άκρης. Τα καλώδια crossover χρησιμοποιούνται για την απευθείας σύνδεση δύο υπολογιστών χωρίς την παρουσία hub ή router. Συγκεκριμένα χρησιμοποιούμε straight through για να συνδέσουμε [174]:

- switch με router
- υπολογιστή με switch
- υπολογιστή με hub

Ενώ χρησιμοποιούμε cross over για να συνδέσουμε:

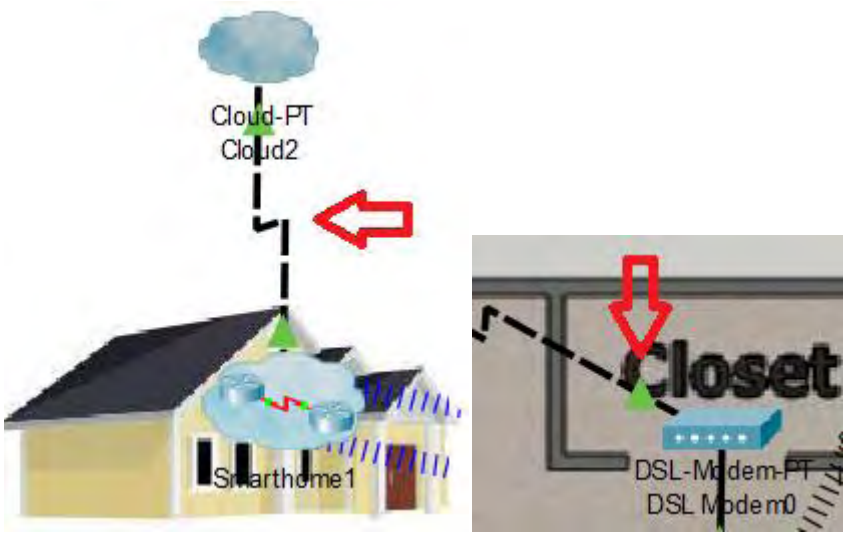
- switch με switch
- switch με hub
- hub με hub
- υπολογιστή με υπολογιστή
- υπολογιστή με router



Crossover (πάνω αριστερά) και Straight Through καλώδια (πάνω δεξιά) [182,183,184]

Τέλος, χρησιμοποιήσαμε την υπάρχουσα τηλεφωνική γραμμή, δηλαδή τα υπάρχοντα καλώδια χαλκού των τηλεφωνικών συνδέσεων για τη σύνδεση ADSL που θέλαμε να προσομοιώσουμε. Το ADSL διαχωρίζει το σήμα σε δύο κανάλια, ένα για φωνή (τηλέφωνο) κι ένα για μεγάλης ταχύτητας σύνδεσης δεδομένων (Internet). Έτσι μπορούμε να συνδεθούμε και στο Internet διότι η τηλεφωνική γραμμή που ξεκινάει από το σπίτι μας καταλήγει στη συσκευή δικτύου DSLAM (Digital Subscriber Line Access Multiplexer). Το σήμα που προκύπτει από

την πολυπλεξία (multiplexing) μεταφέρεται στο δίκτυο του ISP ο οποίος μας δίνει πρόσβαση στο Internet. [185] Για την ADSL σύνδεση μας χρειαστήκαμε μια τηλεφωνική γραμμή και ένα modem router.



Καλώδιο τηλεφωνικής γραμμής στην προσομοίωση

5.4 Δρομολόγηση δικτύου κορμού και IoT επέκτασης

Σε ένα οποιοδήποτε δίκτυο υπολογιστών αυτό που ουσιαστικά γίνεται είναι η μεταφορά μηνυμάτων από τον ένα κόμβο στον άλλο. Σαν κόμβο ονομάζουμε κάθε συσκευή που υπάρχει στο δίκτυο μας όπως, υπολογιστές, tablet, access points, routers, switches κ.α. Ένα μήνυμα λοιπόν από τον ένα κόμβο στον άλλο θα ακολουθήσει μια συγκεκριμένη διαδρομή που θα ξεκινάει από τον κόμβο πηγή και θα καταλήγει στον κόμβο προορισμού. Συνήθως υπάρχουν περισσότερες από μια διαδρομές που μπορεί να ακολουθήσει ένα πακέτο για να φτάσει στον προορισμό του. Η εξεύρεση του «καλύτερου» μονοπατιού λέγεται δρομολόγηση. Σε μικρά δίκτυα, η δρομολόγηση μπορεί να γίνει και χειροκίνητα, δηλαδή στατικά. Σε μεγάλα δίκτυα, που εμπλέκονται πολύπλοκες και διαρκώς μεταβαλλόμενες τοπολογίες, η χειροκίνητη κατασκευή των πινάκων δρομολόγησης είναι προβληματική. Οι αλγόριθμοι δρομολόγησης ουσιαστικά αφορούν τη λεγόμενη δυναμική δρομολόγηση. Ο πίνακας δρομολόγησης είναι μια βάση δεδομένων που βρίσκεται αποθηκευμένη σε έναν δρομολογητή. Οι πίνακες δρομολόγησης χρησιμοποιούνται από τους αλγόριθμους δρομολόγησης, οι οποίοι δίνουν ως αποτέλεσμα τον επόμενο σταθμό στον οποίο πρέπει να μεταφερθεί το πακέτο.

Στην συγκεκριμένη τοπολογία χρησιμοποιήσαμε ένα distance vector πρωτόκολλο που είναι το RIPv2. Τα distance vector πρωτόκολλα ανακοινώνουν σε τακτά χρονικά διαστήματα τα γνωστά σε κάποιον δρομολογητή δίκτυα χωρίς να έχουν γνώση της πλήρους τοπολογίας του δικτύου αλλά μόνο των γειτονικών δρομολογητών. Το RIPv2 χρησιμοποιεί ως παράμετρο μέτρησης (metric) τον αριθμό αλμάτων ενδοκομβικών αποστάσεων, η οποία μετρά την απόσταση μεταξύ της πηγής και του προορισμού (σε άλματα). Ο αριθμός των αλμάτων είναι περιορισμένος με μέγιστο το 15. Χρησιμοποιεί περιοδικά ένα χρονόμετρο timeout (συνήθως κάθε 30 δευτερόλεπτα) για κάθε γνωστή διαδρομή. Αν ο χρόνος αυτός λήξει τότε σημαίνει ότι

το μονοπάτι δεν είναι πλέον διαθέσιμο και ως εκ τούτου ότι η διαδρομή έχει αφαιρεθεί από τους πίνακες δρομολόγησης. Το πρωτόκολο RIP είναι κατάλληλο για τη λειτουργία μικρών δικτύων.

Στους πίνακες δρομολόγησης που προκύπτουν υπάρχουν πληροφορίες για το δρόμο και το κόστος της απόστασης προς τα δίκτυα προορισμού. Ως κόστος χρησιμοποιείται ο αριθμός των ενδιάμεσων δρομολογητών μέχρι να φτάσουμε στο δίκτυο προορισμού (hop count). Στο πρωτόκολλο RIP οι δρομολογητές ανακοινώνουν περιοδικά (κάθε 30 δευτερόλεπτα) ολόκληρο το περιεχόμενο του πίνακα δρομολόγησής τους, στους άμεσα γειτονικούς δρομολογητές. Ο πίνακας δρομολόγησης μπορεί να μεταδοθεί κι όταν υπάρξει κάποια αλλαγή στην τοπολογία του δικτύου. Έτσι επιτρέπεται στο κάθε δρομολογητή να βλέπει το δίκτυο του γειτονικού δρομολογητή και να προσθέτει το ανάλογο κόστος στην απόσταση που έχει ήδη προσθέσει ο δεύτερος.

Το μειονέκτημα της προσέγγισης αυτής είναι ότι καθώς το δίκτυο μεγαλώνει, ανταλλάσσεται ένα μεγάλο ποσό πληροφορίας ανά τακτά χρονικά διαστήματα, ακόμα κι όταν η τοπολογία του δικτύου δεν έχει αλλάξει, με αποτέλεσμα να περιορίζεται το διαθέσιμο εύρος ζώνης και να αυξάνεται ο χρόνος σύγκλισης. Ως χρόνος σύγκλισης (convergence time), ορίζεται ο χρόνος που περνά μέχρι όλοι οι δρομολογητές να συμφωνήσουν σχετικά με την τοπολογία του δικτύου, από τη στιγμή που θα προκύψει μια αλλαγή. Υπάρχουν δυο εκδόσεις του πρωτόκολλου RIP:

- η έκδοση RIP v1, όπου δεν στέλνεται η μάσκα υποδικτύωσης μαζί με τους πίνακες δρομολόγησης (classful routing). Όλα τα δίκτυα πρέπει να έχουν τη default μάσκα και δεν υποστηρίζει VLSM.
- η έκδοση RIP v2, όπου μαζί με τους πίνακες δρομολόγησης στέλνεται και η μάσκα υποδικτύωσης (classless routing), υποστηρίζει VLSM και είναι και η έκδοση που χρησιμοποιήσαμε στην τοπολογία μας [186].

Συγκεκριμένα, με RIPv2 έχουν συνδεθεί οι routers: Router 0, Router 1, Router 2, Router 3, Router 4, Router 6, Router 7, Router 8. Ένα παράδειγμα της παραμετροποίησης τους είναι το εξής αποτέλεσμα που λαμβάνουμε από την εκτέλεση της εντολής «show running-config» που θέσαμε στον Router, ο οποίος έχει οριστεί και ως DHCP client όπως θα δούμε:

```
Router#show running-config
Building configuration...

Current configuration: 1161 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
```

```
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.11.1 255.255.255.0
ip helper-address 192.168.2.2
duplex auto
speed auto
!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/1
no ip address
clock rate 2000000
shutdown
!
interface FastEthernet1/0
ip address 192.168.100.30 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 192.168.2.0
network 192.168.11.0
network 192.168.100.0
no auto-summary
!
```

```
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

Για να επιβεβαιώσουμε ότι έχουμε διαφημίσει όλα τα δίκτυα που γνωρίζει ο Router 4, μπορούμε να του θέσουμε την εντολή «show ip protocols» που θα μας δώσει το εξής αποτέλεσμα:

```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 9 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
Interface Send Recv Triggered RIP Key-chain
FastEthernet1/0 2 2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
192.168.2.0
192.168.11.0
192.168.100.0
Passive Interface(s):
FastEthernet0/0
FastEthernet0/1
Routing Information Sources:
Gateway Distance Last Update
192.168.100.29 120 00:00:25
Distance: (default is 120)
```

Για να μάθουμε ποια δίκτυα «έμαθε» ο Router 4 από τον γείτονα του που είναι ο Router 3 και γενικά να εξετάσουμε αν έχουμε πλήρη επικοινωνία, απλά πληκτρολογούμε την εντολή «show ip route» και παίρνουμε το εξής αποτέλεσμα:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

R 172.16.0.0/16 [120/3] via 192.168.100.29, 00:00:22, FastEthernet1/0
R 172.19.0.0/16 [120/3] via 192.168.100.29, 00:00:22, FastEthernet1/0
R 192.168.0.0/24 [120/3] via 192.168.100.29, 00:00:22, FastEthernet1/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R 192.168.10.0/24 [120/3] via 192.168.100.29, 00:00:22, FastEthernet1/0
C 192.168.11.0/24 is directly connected, FastEthernet0/1
192.168.100.0/30 is subnetted, 9 subnets
R 192.168.100.0 [120/2] via 192.168.100.29, 00:00:22, FastEthernet1/0
R 192.168.100.4 [120/1] via 192.168.100.29, 00:00:22, FastEthernet1/0
R 192.168.100.8 [120/2] via 192.168.100.29, 00:00:22, FastEthernet1/0
R 192.168.100.12 [120/1] via 192.168.100.29, 00:00:22, FastEthernet1/0
R 192.168.100.16 [120/1] via 192.168.100.29, 00:00:22, FastEthernet1/0
R 192.168.100.20 [120/2] via 192.168.100.29, 00:00:22, FastEthernet1/0
R 192.168.100.24 [120/2] via 192.168.100.29, 00:00:22, FastEthernet1/0
C 192.168.100.28 is directly connected, FastEthernet1/0
R 192.168.100.32 [120/2] via 192.168.100.29, 00:00:22, FastEthernet1/0

Με R συμβολίζονται όλα τα δίκτυα που μαθαίνει ο Router 4 χάριν στο πρωτόκολλο RIPv2.

5.5 Ρύθμιση πολιτικών ασφάλειας

Δεδομένης της ιδιαιτέρως ευάλωτης φύσης των ασυρμάτων δικτύων που έχουν καταστεί θύματα συνεχών επιθέσεων, τις περισσότερες φορές με στόχο την απλή υποκλοπή πηγών π.χ. πρόσβαση στο Internet, ρυθμίσαμε μερικά επιπλέον στοιχεία που αθροιστικά μπορούν να βελτιώσουν σημαντικά την ασφάλεια του ασυρμάτου οικιακού δικτύου μας.

Αλλαγή SSID
Το SSID (Service Set Identifier) είναι το όνομα με το οποίο είναι ορατό το δίκτυο του router. Συνήθως το SSID είναι το μοντέλο της συσκευής. Μπορούμε είτε να το αλλάξουμε σε κάτι εντελώς προσωπικό ή να το κάνουμε εντελώς «αόρατο».
Ενεργοποίηση Πρωτοκόλλων Αυθεντικοποιήσης και Κρυπτογράφησης. Προτιμήσαμε το WPA 2 που αποτελεί την ισχυρότερη και πιο αξιόπιστη μορφή για αυθεντικοποίηση και κρυπτογράφηση αυτή τη στιγμή για τα ασύρματα δίκτυα. Σε καμία περίπτωση δεν θα αφήναμε το οικιακό δίκτυο «ξεκλείδωτο», πόσο μάλλον τώρα που αποτελείται από τόσες έξυπνες συσκευές των οποίων η παραβίαση των δεδομένων θα αποτελούσε σοβαρό πλήγμα της ιδιωτικότητας μας. Ακόμη, ενεργοποιήθηκε η τεχνολογία AES (Advanced Encryption Standard), η οποία κρυπτογραφεί αυτά που πληκτρολογούμε πριν από τη μετάδοση τους στον υπολογιστή μας ή σε κάποια άλλη συσκευή. Για να αποτρέπεται η πρόσβαση άλλων ατόμων στο κρυφό κλειδί κρυπτογράφησης AES του πληκτρολογίου μας, το υλικολογισμικό του

AES απαγορεύει την πρόσβαση στο κλειδί αφού αυτό εγκατασταθεί στο πληκτρολόγιο και το δέκτη από το εργοστάσιο.

Ενεργοποίηση του Port Security και MAC Filtering.

Ενεργοποιήσαμε το φίλτρο του Δρομολογητή/Modem, έτσι ώστε μόνο συγκεκριμένες MAC διευθύνσεις να γίνονται αποδεκτές και είναι αυτές των των προσωπικών συσκευών των ιδιοκτητών. Σε περίπτωση που χρειαστεί να συνδεθεί στο δίκτυο της οικίας κάποιος άλλος χρήστης, τότε χειροκίνητα ο administrator και μόνο του δίνει αυτή τη δυνατότητα, πάντα μέσα από κάποιο διαθέσιμο Interface του Δρομολογητή/ Modem.

Απενεργοποίηση του default vlan 1

Για λόγους ασφαλείας, απενεργοποιήσαμε το default native και management vlan 1 του home router και δημιουργήσαμε το vlan 20 στο οποίο αναθέσαμε όλα τα διαθέσιμα interfaces του router σε mode access και απενεργοποιήσαμε το autonegotiation. Επίσης, όσες πόρτες του router δεν χρησιμοποιούνται προς το παρόν, τις απενεργοποιήσαμε

Απενεργοποίηση του DHCP Εξυπηρετητή για άλλα vlan εκτός του vlan 20.

Απενεργοποίηση του DHCP εξυπηρετητή, ώστε ακόμα και αν κάποιος συνδεθεί χωρίς την έγκριση μας στο ασύρματο δίκτυο, να μην λάβει IP διεύθυνση και συνεπώς να είναι αδύνατο να συνδεθεί στο Internet. Εννοείται πως σε αυτή την περίπτωση θα χρειαστεί να δώσουμε εμείς χειροκίνητα IP διεύθυνση στον «ξένο» υπολογιστή και να επιτρέψουμε να χρησιμοποιείται αυτή η διεύθυνση. (Αυτό το μέτρο είναι δύσκολο να εφαρμοστεί σε ένα έξυπνο σπίτι με δυνατότητες επέκτασης του IoT δικτύου με περισσότερες IoT συσκευές, γιατί οι ένοικοι δεν είναι εξασφαλισμένο ότι έχουν τις απαραίτητες γνώσεις για να το κάνουν).

Ενεργοποίηση της δυνατότητας για SSID Cloaking.

Υπάρχει η επιλογή που αναφέρεται ως SSID Broadcast και εμείς μπορούμε να επιλέξουμε Disable. Η σκέψη ήταν να κάνουμε το οικιακό δίκτυο αόρατο απενεργοποιώντας την εκπομπή του SSID του. Έτσι το δίκτυο δεν θα εκπέμπει το όνομα του και για να μπει κάποιος θα πρέπει να του δώσουμε το SSID, όπως προφανώς και τον κωδικό. Καταυτόν τον τρόπο το δίκτυο μας δεν είναι άμεσα ορατό από τους «γείτονες» και δυσκολεύουμε περαιτέρω την προσπάθεια τους να συνδεθούν σε αυτό. Σε αυτό το σημείο, κάτι που έπρεπε να λάβουμε υπόψη μας είναι ότι κάποιες εφαρμογές Wi-Fi, όπως ασύρματες κάμερες ή smart home IoT συσκευές, ίσως να μην λειτουργούν με απενεργοποιημένο το SSID.

Ενεργοποίηση της δυνατότητας για Access Point Isolation.

Συνδεόμαστε στο Router/ Modem μας και αν παρέχει την δυνατότητα, ενεργοποιούμε το Access Point Isolation. Καταυτόν τον τρόπο ακόμη και αν κάποιος κακόβουλος καταφέρει να συνδεθεί στο ασύρματο δίκτυο, δεν έχει την δυνατότητα απευθείας επικοινωνίας με τους άλλους συνδεδεμένους υπολογιστές και συσκευές του δικτύου μας παρά μόνο με το Internet. Ως εκ τούτου διασφαλίζουμε λίγο περισσότερο τα προσωπικά μας δεδομένα.

Περιορισμός της έντασης του σήματος εκπομπής.

Περιορίσαμε την ένταση εκπομπής του σήματος του AP μας, χωρίς να το αφήνουμε να πάει πολύ μακρύτερα από τους τοίχους του δικού μας χώρου. Ως εκ τούτου είναι λιγότερο προσβάσιμο από τους «γύρω» μας.

Μπογιές Ηλεκτρομαγνητικής Θωράκισης (RF Shielding).

Οι τοίχοι βάφονται με κατάλληλη μπογιά και τα παράθυρα καλύπτονται με κατάλληλη αυτοκόλλητη επίστρωση ώστε να περιορίζουν την ένταση του σήματος να «βγαίνει» εκτός του χώρου του σπιτιού.

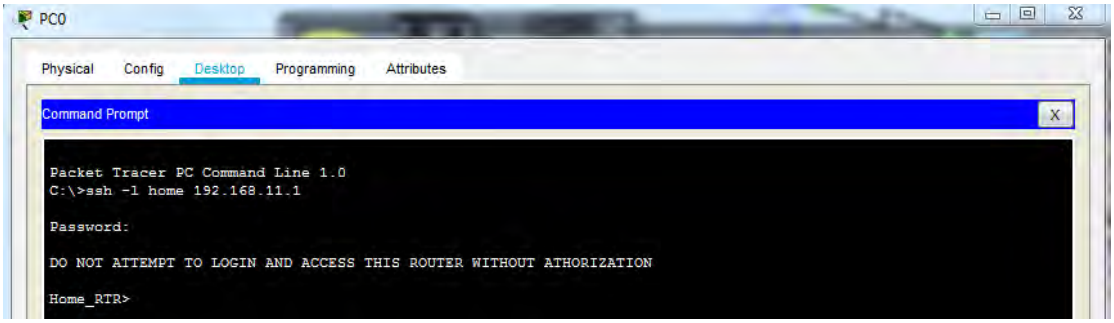
Αλλαγή του κωδικού πρόσβασης διαχειριστή και χρήση δυνατών κωδικών πρόσβασης στον οικιακό router.

Αλλάξαμε τον προεπιλεγμένο κωδικό διαχειριστή και δημιουργήσαμε ένα νέο δυνατό κωδικό για τον δρομολογητή του οικιακού δικτύου. Επίσης συμβουλεύσαμε τους ιδιοκτήτες της οικίας, να αλλάζουν σε τακτά χρονικά διαστήματα τους κωδικούς πρόσβασης, οι οποίοι πρέπει να αποτελούνται από τουλάχιστον 6-8 χαρακτήρες που να περιλαμβάνουν γράμματα, αριθμούς και σύμβολα. Τέλος, να αποφεύγουν να χρησιμοποιούν κοινότυπες λέξεις, όπως ονοματεπώνυμα, emails, αριθμούς τηλεφώνου, κινητού, φαξ και ημερομηνία γέννησης.

Απομακρυσμένη σύνδεση και διαχείριση του οικιακού δικτύου μέσω SSH.

Το SSH είναι ένα πρωτόκολλο που παρέχει ισχυρή από άκρη σε άκρη κρυπτογράφηση για απομακρυσμένη σύνδεση σε υπολογιστές πάνω από μη ασφαλές δίκτυο. Αποτελείται από τρία βασικά στοιχεία:

- Το Transport layer protocol που παρέχει πιστοποίηση της ταυτότητας του server, ακεραιότητα των δεδομένων και εξασφάλιση του απόρρητου της συναλλαγής. Προαιρετικά μπορεί να εφαρμόσει και συμπίεση δεδομένων. Τυπικά τρέχει πάνω από μία TCP/IP σύνδεση.
- Το User Authentication protocol πιστοποιεί την ταυτότητα του πελάτη- χρήστη στον server. Τρέχει πάνω από το Transport layer protocol.
- Το Connection protocol πολυπλέκει το κρυπτογραφημένο φυσικό κανάλι σε αρκετά λογικά κανάλια και τρέχει πάνω από το User Authentication protocol.

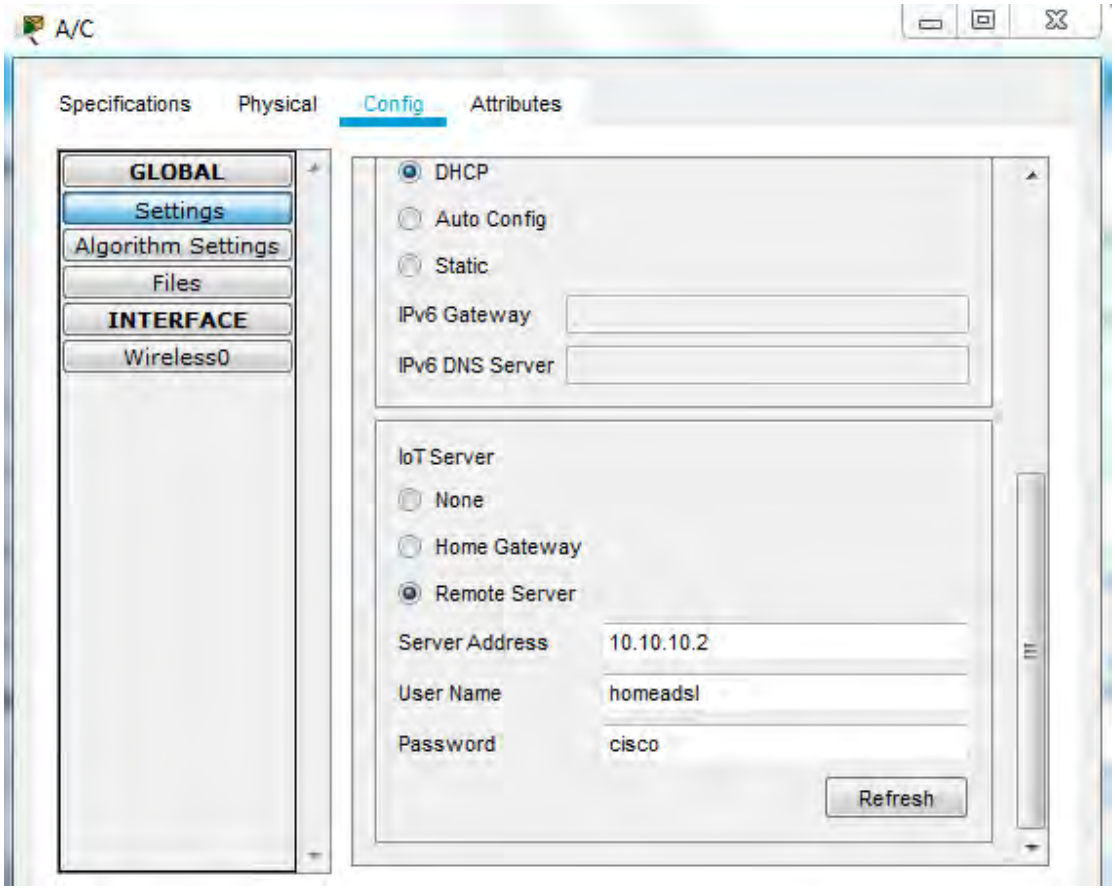


Σύνδεση από το PC του διαχειριστή στον οικιακό ρούτερ

Τα παραπάνω βήματα εξασφαλίζουν σε μεγάλο βαθμό την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του ασύρματου οικιακού δικτύου. Οπωσδήποτε υπάρχουν πολλαπλά αντίμετρα για τον κακόβουλο επιτιθέμενο που μπορεί να ξεπεράσουν πολλά από αυτά τα εμπόδια, π.χ. ειδικές κεραίες λήψης, λήψη πακέτων και έλεγχος IP διευθύνσεων, MAC spoofing κτλ. Παρόλα αυτά, η κεντρική μας ιδέα ήταν να εισάγουμε πολλαπλές διαδοχικές ζώνες άμυνας και να καταστήσουμε το οικιακό δίκτυο ένα μη ελκυστικό στόχο στην συντριπτική πλειοψηφία των εισβολέων ώστε να παραμείνει σε μεγάλο βαθμό ανέπαφο. [214]

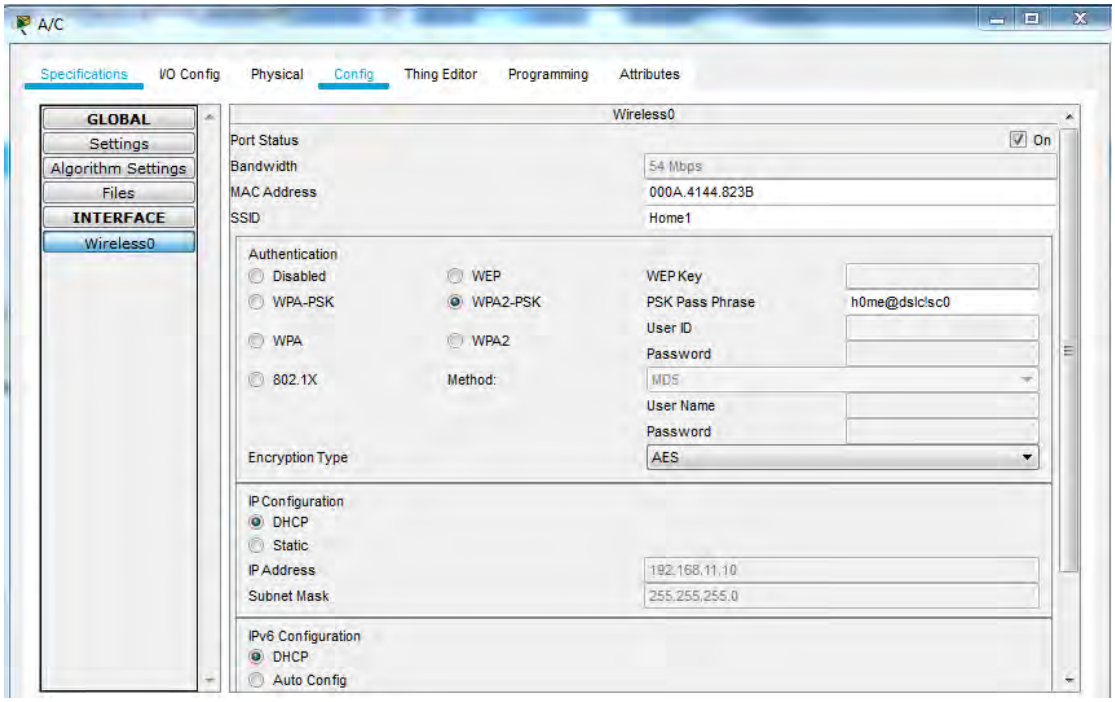
5.6 Παραμετροποίηση IoT συσκευών

Για την προσομοίωση του smarthome 1:
Όπως αναφέρθηκε και νωρίτερα, όλες οι IoT συσκευές και ο IoT server είναι συνδεδεμένοι στο ίδιο WLAN δίκτυο. Η IoT λογική συνδεσιμότητα επιτεύχθηκε συμπληρωματικά της συνδεσιμότητας του δικτύου. Όπως φαίνεται και από την παρακάτω εικόνα, όλες οι IoT συσκευές πρέπει να ρυθμιστούν ώστε να συνδέονται απομακρυσμένα στον IoT server χρησιμοποιώντας τα ήδη ρυθμισμένα: server IP, username και password. Επιτυχημένη σύνδεση θα έχουμε όταν το πεδίο «Connect» αλλάξει σε «Refresh».



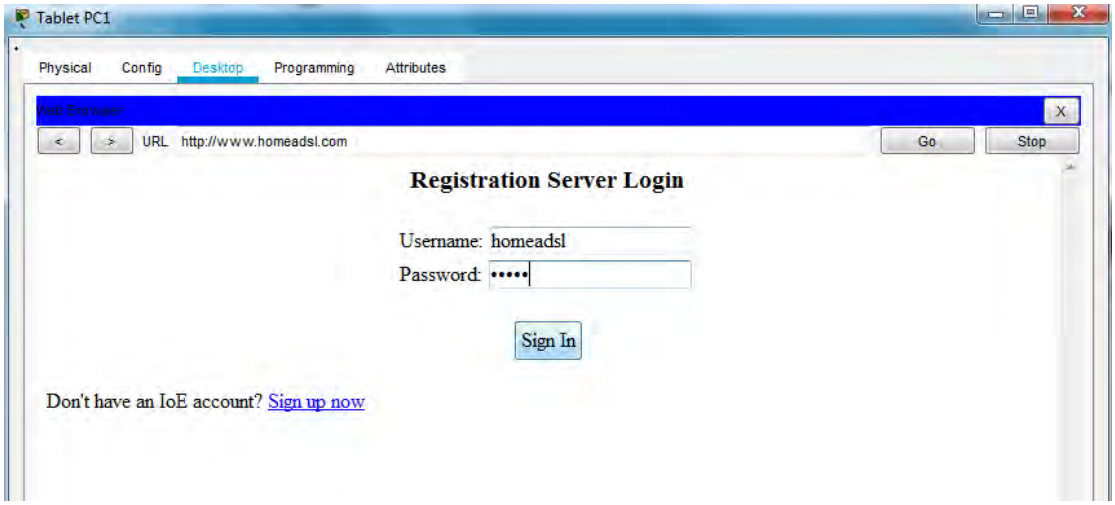
Παράδειγμα του IoT setup του Air Condition

Εφόσον οι έξυπνες συσκευές συνδέονται ασύρματα στο οικιακό LAN μέσω του Access Point, το όνομα δικτύου (SSID) πρέπει να είναι ίδιο με το SSID του σημείου πρόσβασης και αυτό είναι το Home1. Στη συνέχεια, το AP ρυθμίζεται με ένα συγκεκριμένο Pass Phrase (ένα αλφαριθμητικό ASCII από 8 ως 63 χαρακτήρες), το οποίο πρέπει να γνωρίζει ο κάθε client για να μπορέσει να περάσει το authentication και να συνδεθεί στο ασύρματο δίκτυο. Σε αυτό το δίκτυο το Pass Phrase είναι το: h0me@dslc!sc0. Έτσι, όταν ένας client επιλέξει το διαθέσιμο WPA2 δίκτυο και εισάγει το αντίστοιχο Pass Phrase για να συνδεθεί, ο client δημιουργεί το PMK - Pairwise Master Key (ένα κλειδί μήκους 256 bit) και δηλώνει ασύρματα στο AP το ενδιαφέρον του. Ακολουθεί το authentication, μια επικοινωνία τεσσάρων εναλλάξ μηνυμάτων που ξεκινούν από το AP, γνωστή και ως 4-way handshake. Όταν συνδεθεί στο οικιακό LAN, αυτή αλλά και κάθε άλλη συσκευή, θα διευθυνσιοδοτείται από τον DHCP server.



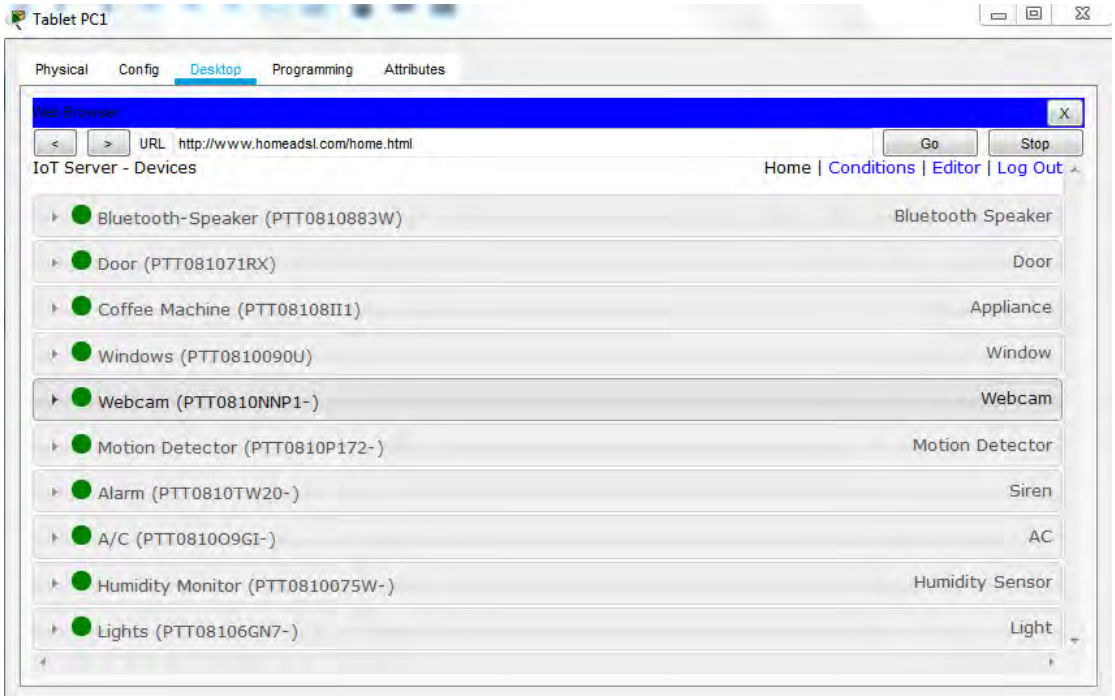
Παράδειγμα ρυθμίσεων που έχουν γίνει στο A/C αλλά και σε κάθε άλλη έξυπνη συσκευή

Όλες οι συσκευές πρέπει να χρησιμοποιούν τα ίδια IoT διαπιστευτήρια. Τα ίδια διαπιστευτήρια χρησιμοποιούνται επίσης και από τους ιδιοκτήτες του smart home ώστε να περάσει την διαδικασία της αυθεντικοποίησης όταν συνδέεται μέσω ενός browser στην κεντρική σελίδα της παρακολούθησης των IoT συσκευών του, όπως φαίνεται στο σχήμα.



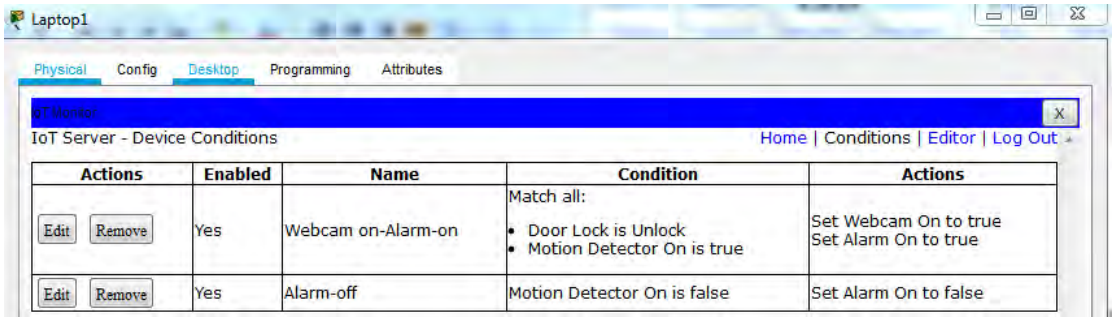
Σύνδεση στο IoT homepage

Όταν ο ιδιοκτήτης συνδεθεί στο homeadsl.com, με username: homeadsl και password: cisco, μπορεί να δει το στάτους των IoT συσκευών του σπιτιού του, τις αλληλεπιδράσεις μεταξύ τους αλλά και να τις ελέγξει.

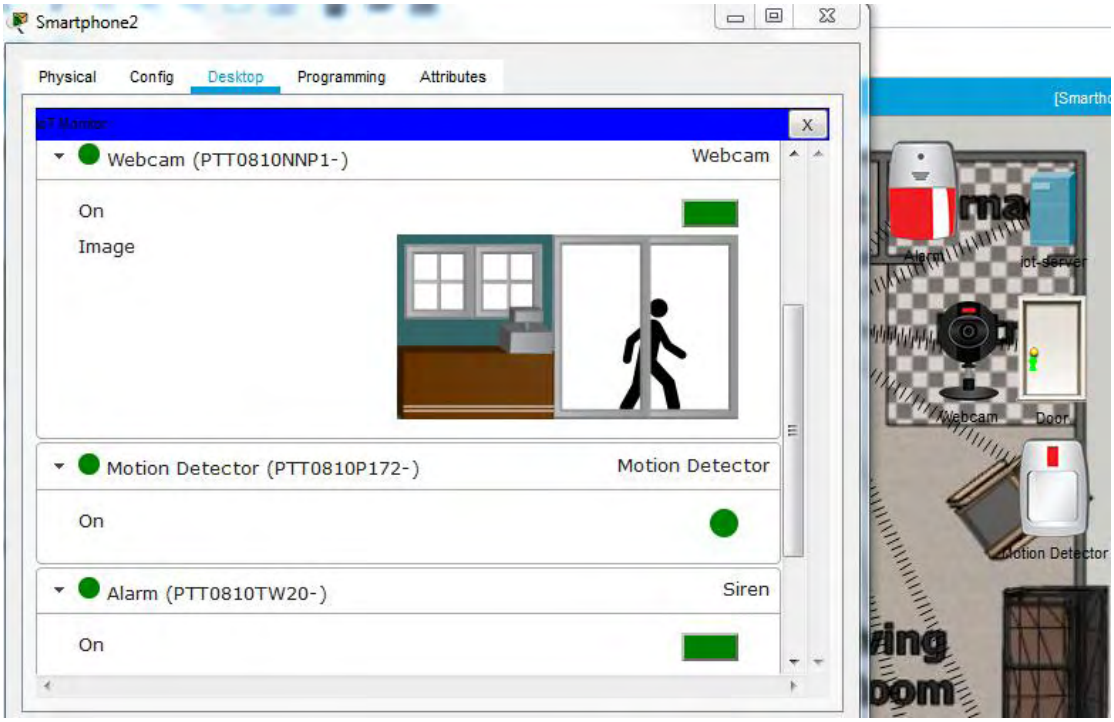


Οι IoT εγγεγραμμένες συσκευές του οικιακού δικτύου

Όπως μπορεί να διαπιστώσει κάποιος, όσο είμαστε συνδεδεμένοι στο IoT homepage μπορούμε να περιηγηθούμε στην καρτέλα «Conditions» και να δούμε ένα βασικό παραδείγματα ρύθμισης και αλληλεπίδρασης των IoT συσκευών μας που αφορά στην ασφάλεια της οικίας. Όπως φαίνεται και από την παρακάτω εικόνα, χρησιμοποιούμε έναν αισθητήρα κίνησης που βρίσκεται εγκατεστημένος εσωτερικά της οικίας, ώστε να ενεργοποιεί προσωρινά τη σειρήνα του συναγερμού του σπιτιού και την webcam. Όταν γίνεται παραβίαση της έξυπνης κλειδαριάς και ο αισθητήρας ανιχνεύσει κάποια κίνηση, τότε θέτει σε λειτουργία τη σειρήνα και την webcam, ενώ όταν ο αισθητήρας δεν ανιχνεύει πια κάποια κίνηση, και μετά από ένα προκαθορισμένο timeout, τότε απενεργοποιεί την σειρήνα, ενώ η webcam μένει ακόμη ανοιχτή για να παρακολουθεί το τι συμβαίνει, σε περίπτωση που οι διαρρήκτες έχουν απενεργοποιήσει τον συναγερμό. Ο ιδιοκτήτης που βρίσκεται εκτός της οικίας, μπορεί να παρακολουθεί τον διαρρήκτη μέσω της εφαρμογής που έχει στο κινητό του.



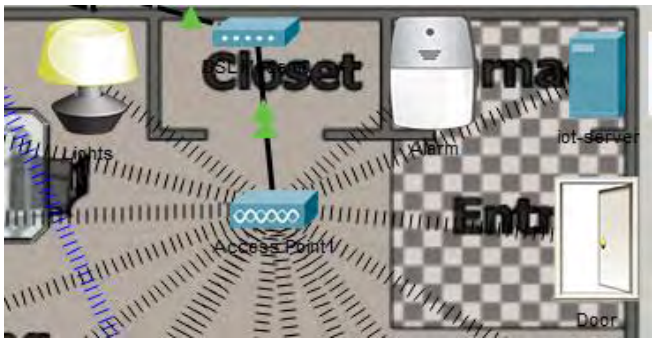
Προκαθορισμένες συνθήκες ρύθμισης ασφαλείας της οικίας



Ενεργοποίηση συναγερμού και webcam μετά από ανίχνευση κίνησης από τον αισθητήρα

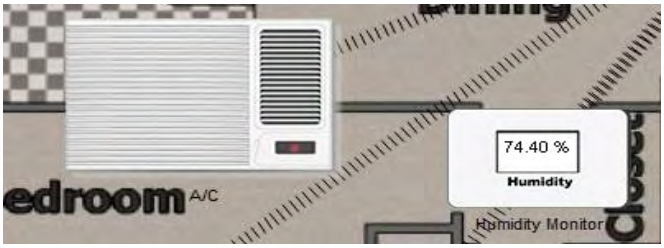
Μια σειρά επιπλέον ρυθμίσεων τύπου IFTTT (If this then that) που έχουν γίνει κατά τη διάρκεια της εγκατάστασης των έξυπνων συσκευών, με χρήση της καρτέλας «Conditions», είναι οι ακόλουθες.

Κάθε φορά που «έξυπνη» εξώπορτα θα είναι ανοιχτή, θα ανάβουν τα φώτα του καθιστικού και της τραπεζαρίας που βρίσκονται πιο κοντά στην είσοδο.



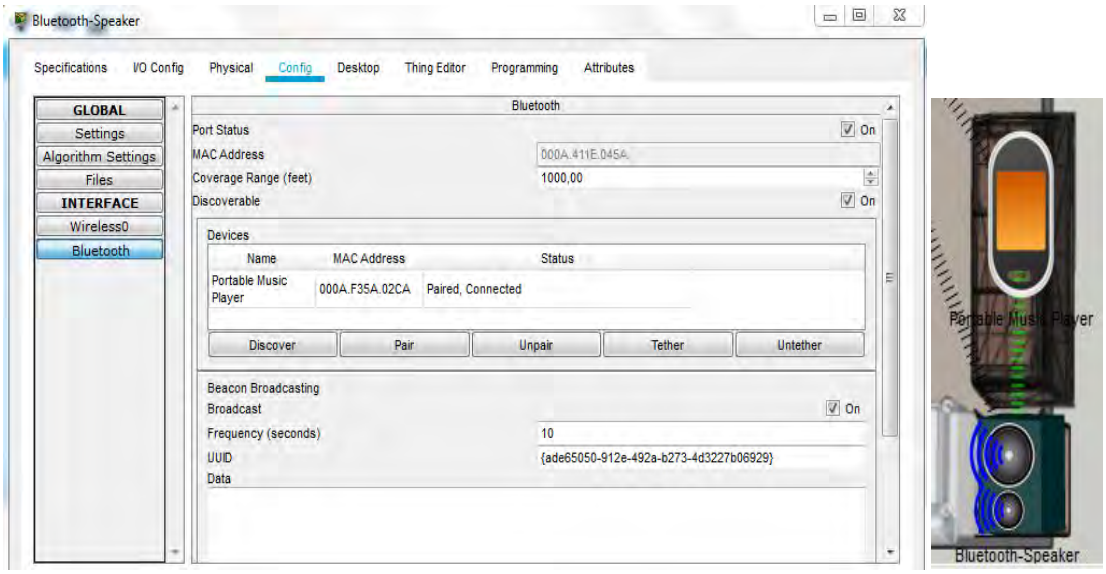
Αλληλεπίδραση φωτισμού και εξώπορτας

Κάθε φορά που το επίπεδο υγρασίας στο εσωτερικό του σπιτιού γίνεται >=50%, ανοίγει το κλιματιστικό, ενώ όταν η υγρασία γίνει <50% τότε το κλιματιστικό κλείνει. Το κλιματιστικό αλληλεπιδρά με τον μετρητή υγρασίας της προσομοίωσης, ελαττώνοντας την υγρασία κατά 2% κάθε μια ώρα.



Η υγρασία βρίσκεται στο 74,4% άρα το A/C έχει ανοίξει

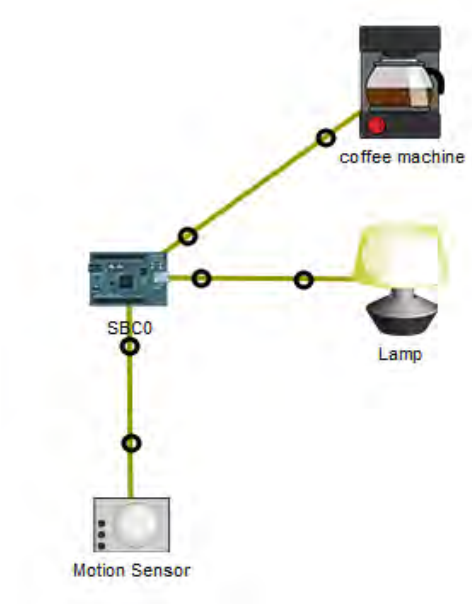
Μια επιπλέον ρύθμιση που έγινε αφορά το οικιακό ηχείο Bluetooth και το φορητό Music Player. Μεταξύ των δύο αυτών συσκευών έγινε η ζεύξη (pairing), ώστε εάν βρίσκονται σε απόσταση 9 μέτρα ≈ 30 ft, το Bluetooth αναλαμβάνει την μεταφορά του ήχου από τη μια συσκευή στην άλλη.



Ζεύξη του φορητού Music Player και του ηχείου Bluetooth και αναπαραγωγή της μουσικής που του μεταφέρει το φορητό Music Player

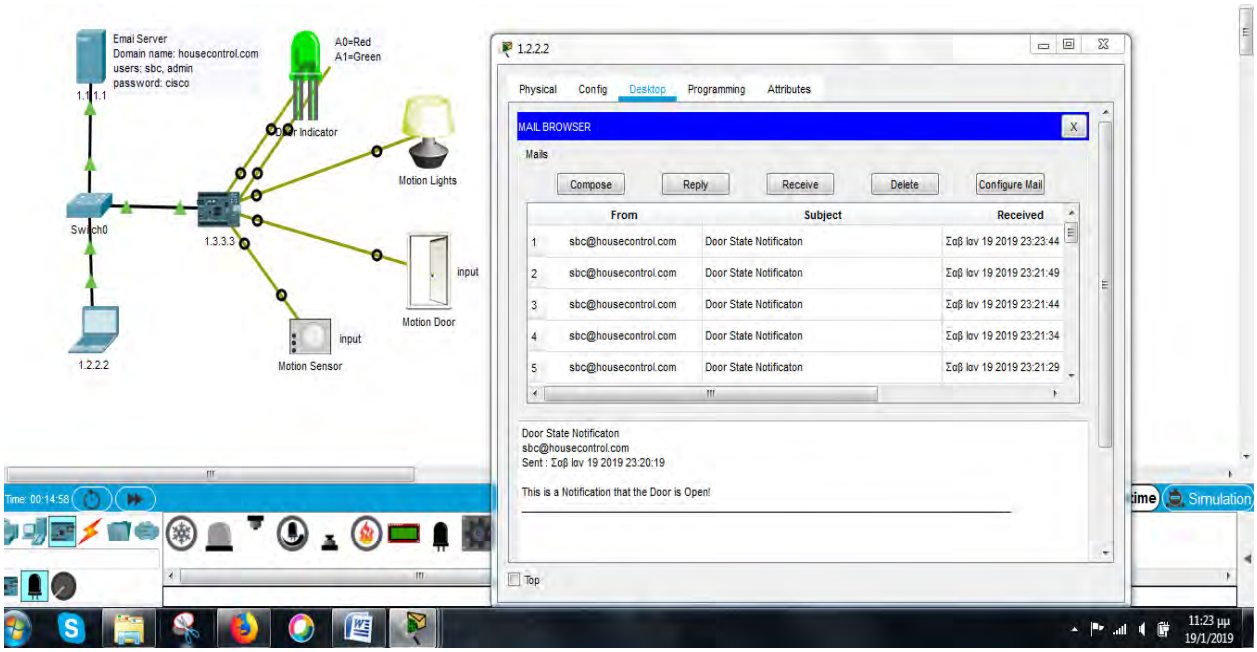
Στη συνέχεια, προτείναμε κάποιους επιπλέον αυτοματισμούς στους ιδιοκτήτες αυτής της οικείας, που θα μπορούσαν να διευκολύνουν ακόμη περισσότερο την καθημερινότητα τους.

Για τον πρώτο αυτοματισμό, χρειαστήκαμε μια έξυπνη καφετιέρα, μια έξυπνη λάμπα, έναν αισθητήρα κίνησης, μια αναπτυξιακή πλακέτα μορφής SBC όπως το Raspberry Pi και custom IoT καλώδια. Η πλακέτα ρυθμίστηκε σε Python ώστε όταν ο αισθητήρας κίνησης θα ανιχνεύει κάποια κίνηση εντός του χώρου της κουζίνας, θα ανάβει την έξυπνη λάμπα της κουζίνας και θα ανάβει και την καφετιέρα, όπως φαίνεται στην παρακάτω εικόνα.



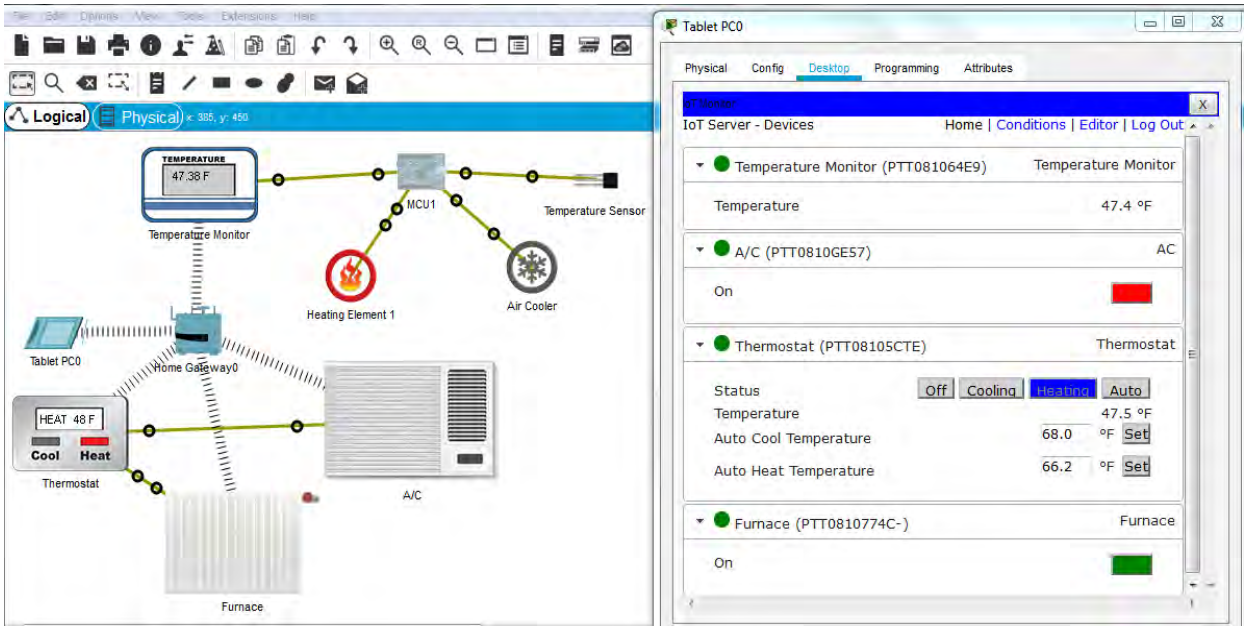
Αναπαράσταση του αναφερθέντος κυκλώματος στην προσομοίωση

Για τον δεύτερο αυτοματισμό, χρειαστήκαμε έναν email server, ένα switch, ένα RGB led, μια έξυπνη λάμπα, έναν αισθητήρα κίνησης που τοποθετείται πάνω στην πόρτα, μια αναπτυξιακή πλακέτα μορφής SBC όπως το Raspberry Pi και custom IoT καλώδια. Η πλακέτα ρυθμίστηκε ώστε κάθε φορά που ο αισθητήρας που βρίσκεται πάνω στην πόρτα (δεδομένου ότι η πόρτα είναι ξεκλείδωτη), θα ανιχνεύει κάποια κίνηση η εξώπορτα θα ανοίγει αυτόματα, το RGB led θα γίνεται πράσινο (δηλαδή θα δηλώνει ότι η πόρτα είναι ανοιχτή), θα ανάβουν τα φώτα της εισόδου και θα στέλνεται email απευθείας στους ιδιοκτήτες για την κατάσταση της πόρτας, όπως δείχνει η παρακάτω εικόνα. Όταν ο αισθητήρας δεν ανιχνεύει πια κάποια κίνηση, και μετά από ένα προκαθορισμένο timeout, τότε απενεργοποιεί τα φώτα της εισόδου και το RGB led και κλείνει την πόρτα. Ο email server ρυθμίστηκε ώστε να εκτελεί τις υπηρεσίες SMTP και POP3. Τέλος, αυτός ο αυτοματισμός επιτελεί τον σκοπό της καθημερινής ευκολίας για την είσοδο και την έξοδο από το σπίτι και επίσης είναι ιδιαίτερα χρήσιμος σε περίπτωση που στην οικία κατοικεί άτομο με κάποια αναπηρία.



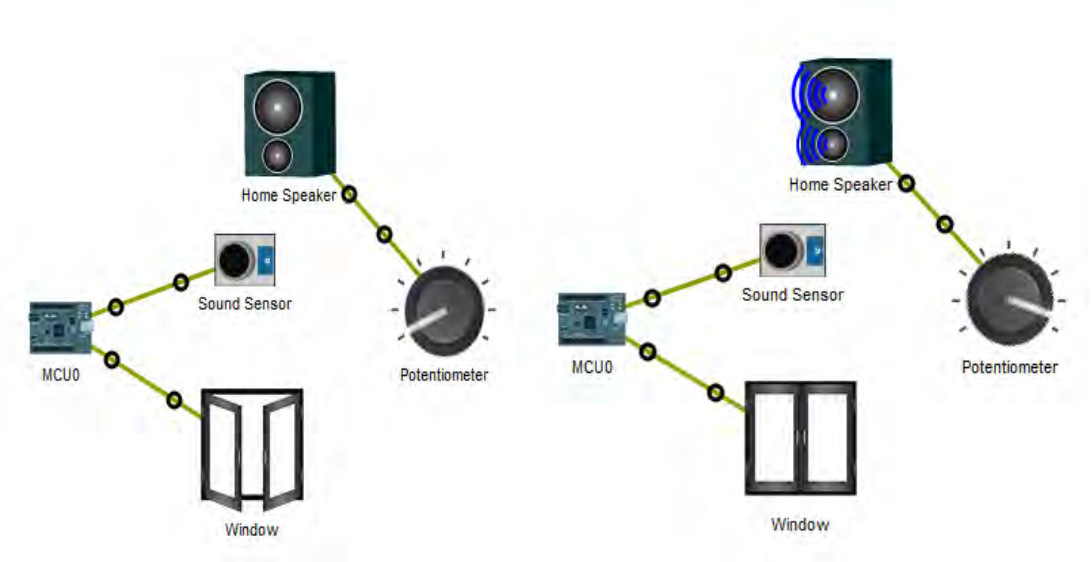
Ο ιδιοκτήτης έλαβε email για την κατάσταση της πόρτας

Για τον τρίτο αυτοματισμό χρειαστήκαμε έναν αισθητήρα θερμοκρασίας, έναν θερμοστάτη, μια ψηφιακή οθόνη θερμοκρασίας, ένα κλιματιστικό, ένα σώμα θέρμανσης, έναν μικροελεγκτή, από έναν ενεργοποιητή θέρμανσης και ψύξης και custom IoT καλώδια. Ο μικροελεγκτής προγραμματίστηκε σε JavaScript ώστε να λαμβάνει από τον αισθητήρα θερμοκρασίας τη θερμοκρασία του περιβάλλοντος και να την εμφανίζει στην ψηφιακή οθόνη θερμοκρασίας. Οι ιδιοκτήτες του σπιτιού μπορούν να έχουν τον απόλυτο έλεγχο της θερμοκρασίας της οικείας μέσω του IoT Monitor ενός tablet.



Έλεγχος της θερμοκρασίας της οικίας μέσω του IoT monitor

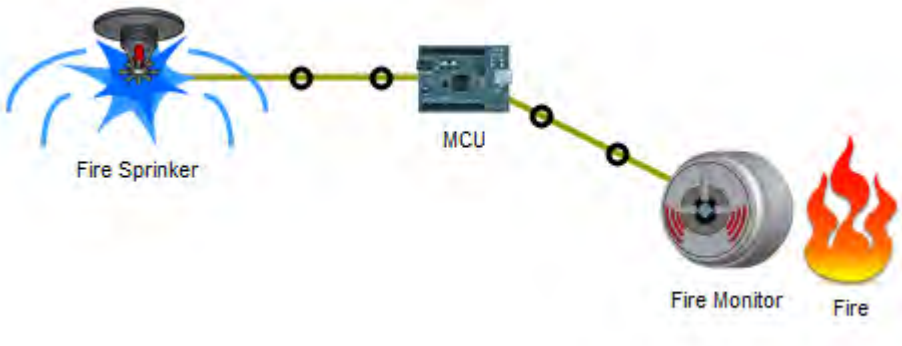
Για τον τέταρτο αυτοματισμό χρειαστήκαμε έναν μικροελεγκτή και έναν αισθητήρα ήχου. Ο μικροελεγκτής προγραμματίστηκε σε JavaScript ώστε αν τα έξυπνα παράθυρα της οικίας είναι ανοιχτά και το ηχείο αναπαράγει ήχο μεγαλύτερο από 65 dB να κλείσει αμέσως τα παράθυρα, ενώ αν ο ήχος είναι κάτω από 50 dB τα παράθυρα ξανά ανοίγουν.



Τα έξυπνα παράθυρα της οικίας κλείνουν και ανοίγουν ανάλογα με τα dB

Για τον τελευταίο αυτοματισμό, χρειαστήκαμε έναν μικροελεγκτή, ένα πυροσβεστικό σύστημα καταιονισμού, έναν αισθητήρα φωτιάς και custom IoT καλώδια. Για την προσομοίωση επιπλέον χρειάστηκε να προγραμματίσουμε ένα Thing 

σε JavaScript ώστε να του αποδώσουμε την ιδιότητα της φωτιάς μέσω της συνάρτησης setDeviceProperty(getName(), 'IR', 900); (Το component "Fire" δεν υπάρχει στην έκδοση του Packet Tracer που χρησιμοποιήσαμε, γι αυτό και χρειάστηκε να το δημιουργήσουμε). Ο αισθητήρας ανιχνεύει τις φλόγες ελέγχοντας την τιμή της ιδιότητας IR και ενεργοποιεί αναλόγως το σύστημα πυρόσβεσης.



Ο αισθητήρας ανίχνευσε τα επίπεδα IR και έθεσε σε λειτουργία το σύστημα πυρόσβεσης

Κεφάλαιο 6: Συμπεράσματα

Προσπαθώντας να αναλύσουμε το κόστος της αρχιτεκτονικής ενός έξυπνου σπιτιού θα λέγαμε πως στην πραγματικότητα είναι φθηνότερο σε σύγκριση με ένα συμβατικό αν η κατασκευή του γινόταν «έξυπνη» εξαρχής. Αυτή η αναφορά γίνεται στο γενικό όφελος για τον ιδιοκτήτη, το κράτος και τον πλανήτη και στην ενέργεια η οποία εξοικονομείται. Επίσης, υπάρχει και η πρακτική παράμετρος. Η κατασκευή ενός έξυπνου σπιτιού δεν κοστίζει περισσότερο από ένα συμβατικό σε ότι αφορά στα υλικά κατασκευής. Τα ίδια υλικά θα χρησιμοποιηθούν και στα δύο σπίτια. Το ίδιο μπετόν, τα ίδια τούβλα και τα ίδια κουφώματα θα μπουν και στη μια και στην άλλη περίπτωση. Σύγχυση κυρίως παρατηρείται στο αν χρειάζεται θερμομόνωση ή όχι στα μπετά της οικοδομής, καθώς η θερμομόνωση επιβαρύνει χρηματικά την κατασκευή μέχρι και 5%. Το πραγματικό κόστος μιας οικοδομής, εξαρτάται από το κόστος κατασκευής κατά 20-25% και από το κόστος λειτουργίας στο χρόνο ζωής του κτιρίου κατά 75-80%. Έτσι αν η θερμομόνωση αυξάνει το κόστος κατασκευής κατά 5%, αυξάνει το πραγματικό κόστος του κτιρίου μόνο κατά 1%. Όμως, αν γίνει σωστή θερμομόνωση στην κατασκευή και μειωθεί η σπατάλη ενέργειας στο κτίριο έως και 50%, τότε εξασφαλίζουμε οικονομία 40% στο συνολικό πραγματικό κόστος της οικοδομής και πετυχαίνουμε εξοικονόμηση ενέργειας για τον ιδιοκτήτη, τη χώρα και τον πλανήτη.

Όσο για τα πλεονεκτήματα των ηλεκτρολογικών εγκαταστάσεων μιας έξυπνης οικίας από μια συμβατική είναι ότι αποτελούν εγγύηση για το μέλλον, μιας και η επέκταση της εγκατάστασης γίνεται χωρίς περιορισμούς και είναι πλήρως προσαρμόσιμη σε τυχόν αλλαγές της εγκατάστασης ή επεκτάσεις στο μέλλον. Επίσης λόγω της αυτοματοποίησης της εγκατάστασης, δηλαδή του ελέγχου του φωτισμού και της θέρμανσης κατά τη διάρκεια απουσίας των ιδιοκτητών, συντελείται μείωση των εξόδων χρήσης της εγκατάστασης και προστασία του περιβάλλοντος χάρη στον περιορισμό της έκλυσης άνθρακα στην ατμόσφαιρα. Ο χειρισμός είναι πιο απλοποιημένος, γίνεται οικονομική διαχείριση της ενέργειας, αυξάνεται η ασφάλεια των χρηστών και της οικίας με αποτέλεσμα τη διαφύλαξη της επένδυσης. Τέλος προσφέρεται άνετη διαβίωση που συντελεί και στην αύξηση της αξίας της οικίας σε περιπτώσεις ενοικίασης ή πώλησης.

Αν κι έχουν σημειωθεί μεγάλες τεχνολογικές εξελίξεις από την πρώτη εμφάνιση του έξυπνου σπιτιού πάνω από τριάντα χρόνια πριν, το ευρύ καταναλωτικό κοινό, ο μέσος καταναλωτής, δεν δείχνει να αποδέχεται το έξυπνο σπίτι σε ικανοποιητικό βαθμό. Ο συνδυασμός που κινεί το μέσο καταναλωτή να επενδύσει σε ένα νέο τεχνολογικό προϊόν, όπως το έξυπνο σπίτι, βρίσκεται στη χρυσή τομή μεταξύ κόστους, αναγκαιότητας και γούστου. Κάθε νέα τεχνολογία είναι ενδιαφέρουσα και τραβάει την προσοχή, αλλά εάν η ίδια της η εφαρμογή κρίνεται μη χρήσιμη ή ακριβή, οι καταναλωτές δεν θα την προτιμήσουν. Αν θελήσει κανείς να υλοποιήσει ένα έξυπνο σπίτι με την τελευταία λέξη της τεχνολογίας θα αντιμετωπίσει πολύ υψηλά κόστη. Προς το παρόν, ο καταναλωτής έχει δείξει να φοβάται τις δυσκολίες που μπορεί να προκύψουν κατά την εγκατάσταση και τη συντήρηση, καθώς και πιθανές ασυμβατότητες που ίσως προκύψουν μεταξύ του εξοπλισμού. Ο καταναλωτής επίσης δείχνει να προσδοκεί ακόμη μεγαλύτερες εξελίξεις γύρω από το έξυπνο σπίτι στο άμεσο μέλλον, γεγονός που τον κάνει να αναμένει νέες αλλαγές στην αγορά προτού κινηθεί.

Αν θέλουμε να αλλάξουμε αυτό το στατικό κλίμα θα πρέπει να δοθεί έμφαση στη χρηστικότητα και τη λειτουργικότητα του έξυπνου σπιτιού, καθώς και στη φιλικότητα προς το χρήστη. Η τεχνολογία πρέπει να γίνει οικεία και γνωστή στο χρήστη. Αν μπορέσουμε να δώσουμε στο καταναλωτικό κοινό σαφή εικόνα γύρω από τον τρόπο λειτουργίας του έξυπνου σπιτιού, το κλίμα στην αγορά θα βελτιωθεί. Το έξυπνο σπίτι ήρθε για να κάνει τη ζωή μας πιο απλή και εύκολη και όχι πιο περίπλοκη.

Άλλο ένα μείζον θέμα είναι ότι η μεγαλύτερη μερίδα χρηστών κατέχουν ήδη ένα σπίτι και είναι λογικό να είναι πιο δύσκολο και κοστοβόρο να τροποποιήσουν ένα υπάρχον σπίτι στο να γίνει έξυπνο σε σχέση με το να δημιουργήσουν ένα έξυπνο σπίτι από τα θεμέλια. Κατά τη διαδικασία προκύπτουν πρόσθετα κόστη διότι χρειάζεται πρόσθετος χρόνος ρυθμίσεων και τροποποιήσεων. Μπορεί τα σημερινά σπίτια να διαθέτουν κάποια από τα στοιχεία που χρειάζεται ένα έξυπνο σπίτι (όπως πρόσβαση στο Internet, ηλεκτρονικούς υπολογιστές, κινητά τηλέφωνα, σύγχρονες τηλεοράσεις κ.ά.), ωστόσο, ακόμη και έτσι υπολείπονται αρκετών δομών και χαρακτηριστικών που είναι απαραίτητα (όπως δίκτυα αισθητήρων, διεπιφάνειες χρήστη, ειδικό λογισμικό, πρόσθετα τερματικά κ.ά.).

Η Gartner πραγματοποίησε μια έρευνα γύρω από το θέμα της αποδοχής της τεχνολογίας του έξυπνου σπιτιού από το κοινό [219]. Η έρευνα κατέδειξε ως κύρια αιτία για την αντίσταση του αγοραστικού κοινού, την απουσία συμβατότητας μεταξύ των συσκευών και των επιμέρους δικτύων, δηλαδή την έλλειψη κοινών προτύπων στο χώρο. Οι υψηλές τιμές αποδείχτηκε ότι επηρεάζουν αρνητικά το χρήστη, αλλά σε μικρότερο βαθμό από το αναμενόμενο. Επιπλέον, θέματα ασφάλειας και ιδιωτικότητας φάνηκε ότι προβληματίζουν σοβαρά το αγοραστικό κοινό. Οι κάμερες, οι αισθητήρες και οι άλλοι μηχανισμοί που βρίσκονται μέσα στο έξυπνο σπίτι συγκεντρώνουν πολλά προσωπικά δεδομένα για το χρήστη, γεγονός που δημιουργείανασφάλεια και ανησυχία. Τα κενά ασφαλείας που έχουν παρουσιαστεί κατά καιρούς στο Internet και οι διάφορες επιθέσεις hacking που έχουν καταγραφεί βρίσκονται πίσω από το φόβο του μέσου χρήστη. Είναι σημαντικό λοιπόν, οι δομές μέσα στο έξυπνο σπίτι να είναι στιβαρές και το σύστημα να είναι πλήρως προφυλαγμένο από εξωτερικές απειλές, ακόμη και αν χρειαστεί να θυσιαστεί κομμάτι της λειτουργικότητας που τελικά προσφέρεται. Αυτό που αξίζει να τονιστεί είναι πως αν θέλουμε το έξυπνο σπίτι να αποτελέσει στο άμεσο μέλλον κομμάτι της καθημερινότητας μας θα πρέπει να μεταφέρουμε τη διαδικασία σχεδίασης και ανάπτυξης από τα εργαστήρια στα πραγματικά σπίτια. Οι κάτοικοι του εκάστοτε σπιτιού θα πρέπει να γίνουν στην πράξη, έστω με έμμεσο τρόπο, οι πραγματικοί σχεδιαστές του, διαφορετικά όσο καλό και να είναι ένα σύστημα έξυπνου σπιτιού ποτέ δε θα γίνει πλήρως επιθυμητό και αποδεκτό.

Με τις εξελίξεις στην περιοχή των αισθητήρων, πρωτοκόλλων και τεχνολογιών αποθήκευσης ενέργειας, τα δίκτυα αισθητήρων αποτελούν τον πυρήνα του IoT. Σε συνδυασμό με το υπολογιστικό νέφος (Cloud) και την επεξεργασία μεγάλων δεδομένων (Big Data), οι δυνατότητες πλέον είναι απεριόριστες σε αυτόν τον τομέα και οι χρήστες θα μπορούν να ελέγχουν τα περιβάλλοντα που ζουν και δρουν καθημερινά με εύκολο τρόπο. Μερικοί παράγοντες που σχετίζονται με τα WSN που χρήζουν περαιτέρω προσοχής στο μέλλον είναι οι παρακάτω:

Κόστος: Μια λύση χαμηλού κόστους είναι πάντα επιθυμητή για την αύξηση του πεδίου εφαρμογής που ισοδυναμεί με αύξηση της πιθανότητας εντοπισμού του επιθυμητού γεγονότος που μελετάται.

Αυτόνομη λειτουργία: Οι μελλοντικές λύσεις πρέπει να περιλαμβάνουν τη πρόβλεψη για αυτόνομες επιχειρήσεις που επιβιώνουν για μεγάλο χρονικό διάστημα.
Νοημοσύνη: Μια εγγενής νοημοσύνη, η οποία θα επιτρέψει στις φουτουριστικές λύσεις να αντιδράσουν δυναμικά σε πολλαπλές προκλήσεις, από την εξοικονόμηση ενέργειας στην απόκριση σε πραγματικό χρόνο.
Φορητότητα: Η φορητότητα του συστήματος, για εύκολη εφαρμογή είναι ουσιώδης. Πρόσφατες εξελίξεις στα ενσωματωμένα συστήματα, όπως το System in Package (SiP) και το System on Chip (SoC) συντελούν στην άποψη αυτή.
Χαμηλή συντήρηση: Είναι απαραίτητο να σχεδιαστεί ένα σύστημα το οποίο απαιτεί ελάχιστη προσπάθεια συντήρησης. Αυτό ασφαλώς θα ελαχιστοποιήσει το μέσο κόστος μακροπρόθεσμα.
Ενεργειακή απόδοση: Για να εξασφαλιστεί η εκτεταμένη διάρκεια ζωής με αυτονομία, οι λύσεις πρέπει να είναι πιο ενεργειακά αποδοτικές ενσωματώνοντας ευφυείς αλγορίθμους.
Ισχυρή αρχιτεκτονική: Μια ισχυρή αρχιτεκτονική ανθεκτική στο σφάλμα, στις νεοεμφανιζόμενες εφαρμογές, είναι απαραίτητη για την εξασφάλιση βιωσιμότητας της λειτουργίας.
Εύκολη λειτουργία: Συνήθως, οι τελικοί χρήστες αυτών των εφαρμογών είναι μη τεχνικά πρόσωπα. Επομένως, αυτές οι εφαρμογές χρειάζονται να είναι απλές και εύκολες στη χρήση.
Διαλειτουργικότητα: Διαλειτουργικότητα μεταξύ των διαφόρων στοιχείων και των διαφορετικών τεχνολογιών επικοινωνιών θα ενισχύσουν τη συνολική λειτουργικότητα του συστήματος.

Επίσης, καθοριστικές θα είναι και οι εξελίξεις των WSN όσον αφορά στις νέες τεχνικές δρομολόγησης που θα έχουν στόχο την επέκταση της διάρκειας ζωής τους, την εξοικονόμηση ενέργειας και την προσαρμοστικότητα τους σε απροσδόκητες περιβαλλοντικές συνθήκες. Κάποιες από αυτές αφορούν το network clustering, τις τεχνικές για fault tolerance, την ενδοδικτυακή κατανεμημένη επεξεργασία των δεδομένων, το σύστημα εντοπισμού των κόμβων αισθητήρων (καθώς το GPS δεν μπορεί να χρησιμοποιηθεί γι αυτό το σκοπό), την αυτό-διαμόρφωση σε δυναμικά συστήματα WSN, την ασφάλεια κ.ά. [220]

Το 2018 υπήρξε μια σημαντική χρονιά για το έξυπνο σπίτι, με προόδους στο πώς μπορούμε να διαχειριστούμε διάφορες έξυπνες συσκευές. Έχουμε δει την Alexa της Amazon και τον Google Assistant να προσφέρουν έλεγχο των συσκευών μέσω ηχείων, έτσι μπορούμε απλά να πούμε "άναψε το φως" και να καταλάβει το σύστημα μας τι εννοούμε. Το Apple HomeKit έχει αρκετές βελτιώσεις, τόσο με τον καλύτερο χειρισμό μέσω της εφαρμογής, όσο και με τον έλεγχο φωνής μέσω του εξαιρετικού HomePod. Παρ 'όλα αυτά, δεν έχουμε φτάσει στον τελικό στόχο ακόμη. Καθώς βλέπουμε το νέο έτος, υπάρχουν τέσσερις τρόποι με τους οποίους το έξυπνο σπίτι μπορεί να βελτιωθεί το 2019.

Περισσότερη διαλειτουργικότητα

Αν θέλουμε όλες οι έξυπνες οικιακές συσκευές μας να ελέγχονται μέσω μιας μόνο διασύνδεσης, αυτό ακόμη δεν είναι εφικτό. Η υποστήριξη για την Apple Home, SmartThings, Alexa και το Google Home ποικίλλει, χωρίς ένα ενιαίο σύστημα που να προσφέρει υποστήριξη σε όλες τις συσκευές. Επιπλέον, υπάρχουν αυτή τη στιγμή περιπτώσεις στις οποίες εταιρείες αρνούνται ακόμη και την υποστήριξη. Ας πάρουμε για παράδειγμα το Nest Thermostat E, το οποίο βγήκε στην αγορά χωρίς να υποστηρίζει την Alexa της Amazon. Επίσης, η Google δεν θα υποστηρίξει το Apple HomeKit για οποιαδήποτε συσκευή Nest. Προκειμένου το έξυπνο σπίτι να

συνεχίσει να αναπτύσσεται, χρειάζεται να υπάρχει ευρύτερη υποστήριξη για συσκευές από τα μεγαλύτερα συστήματα φωνής-ήχου και καλύτεροι τρόποι για να επικοινωνούν οι συσκευές μεταξύ τους.

Ευκολότερος αυτοματισμός (αυτοματοποίηση)

Το επόμενο στάδιο ενός έξυπνου σπιτιού είναι η αυτοματοποίηση, όπως η ενεργοποίηση του φωτισμού αυτόματα τη νύχτα όταν ανοίγουμε την μπροστινή μας πόρτα ή απενεργοποιώντας τα πάντα όταν βγαίνουμε έξω. Ενώ ήμερα είναι δυνατόν να δημιουργηθεί ένα τέτοιο επίπεδο ελέγχου, δεν είναι πάντα εύκολο. Με το SmartThings για παράδειγμα, η ρύθμιση διαφορετικών αυτοματισμών με βάση την ώρα της ημέρας απαιτεί πρώτα να δημιουργήσουμε πολλαπλές καταστάσεις-λειτουργίες και, στη συνέχεια, να δημιουργήσουμε πρόσθετους κανόνες στην κορυφή αυτών. Είναι ένα κανονικός λαβύρινθος για να γίνουν όλα τα βήματα με τη σωστή σειρά. Το Amazon ενισχύει τις λειτουργίες του Alexa Routine με τον Έλεγχο Θέσης, κάτι που θα μπορούσε να βελτιώσει πολλά θέματα εδώ, αλλά το ίδιο σύστημα δεν διαθέτει το ίδιο επίπεδο ελέγχου αλλού.

Πιο αξιόπιστοι έλεγχοι από άλλους κατασκευαστές

Οι συσκευές άλλων κατασκευαστών που χρησιμοποιούνται για τον έλεγχο του έξυπνου σπιτιού δεν λειτουργούν πάντα τόσο καλά όσο θα περίμενε κανείς. Για παράδειγμα, είναι αρκετά συχνό να ζητήσουμε από την Alexa να ενεργοποιήσει τα φώτα του σπιτιού μας αλλά το μόνο που θα δούμε είναι, το μπλε της φως που περιστρέφεται πριν αποτύχει να εκτελέσει την εντολή μας. Μια δεύτερη προσπάθεια θα λειτουργήσει, συνήθως. Ομοίως, υπάρχουν στιγμές όπου είναι ευκολότερο να πάμε και να πατήσουμε ένα διακόπτη από το να χρησιμοποιήσουμε τη φωνή μας ή μια εφαρμογή. Ωστόσο, μερικά συστήματα έχουν φυσικούς ελέγχους, με τη Philips Hue να είναι η αξιοσημείωτη εξαίρεση. Οι επιλογές από άλλους κατασκευαστές, όπως το Flic Hub ή το Logitech Pop, παρέχουν φυσικούς διακόπτες, αλλά δεν είναι πάντα αξιόπιστα, για παράδειγμα, έχει αναφερθεί πρόβλημα να μην ενεργοποιούνται όλες οι λυχνίες Hue ή ένας έξυπνος διακόπτης μπορεί να αργήσει αρκετά να δράσει. Μέρος του προβλήματος είναι ότι οι συσκευές από άλλους κατασκευαστές πρέπει να ελέγχουν από απόσταση μια έξυπνη οικιακή συσκευή ή μέσω ενός API, το οποίο τείνει να είναι λιγότερο αξιόπιστο από την άμεση μέθοδο που χρησιμοποιείται από την επίσημη εφαρμογή. Το άνοιγμα των συστημάτων σε άλλους κατασκευαστές θα μπορούσε να βελτιώσει δραματικά την αξιοπιστία των κουμπιών, προσφέροντας περισσότερη εμπιστοσύνη για μελλοντική μετάβαση από τον ενσύρματο στον ασύρματο έλεγχο.

Ευφυέστερη συντήρηση

Το έξυπνο σπίτι δεν πρέπει μόνο να αφορά τον έλεγχο των συσκευών, θα πρέπει επίσης να δίνει περισσότερες πληροφορίες για τη διαχείριση της συντήρησης. Η LG έχει ήδη ενσωματώσει το ThinQ σε ορισμένες από τις high-end συσκευές της, με το σύστημα να μας ειδοποιεί για τυχόν προβλήματα. Για παράδειγμα, «το ψυγείο σας δεν ψύχεται σωστά». Πρέπει να δούμε στο μέλλον περισσότερες από αυτές τις καινοτομίες, με τους αισθητήρες να παρακολουθούν και να επιβλέπουν τις οικιακές συσκευές μας και να μας λένε για προβλήματα προτού να καταστούν μοιραία. Αυτό το είδος προληπτικής συντήρησης μπορεί να επιταχύνει τις επισκευές, ενώ οι τεχνικοί υπάλληλοι της υπηρεσίας μπορούν να εμφανιστούν άμεσα με τα σωστά εξαρτήματα για επισκευή. Η Tado εξετάζει το πώς μπορεί να χρησιμοποιήσει μια ψηφιακή

διεπαφή του λέβητα (OpenTherm) για να συλλέξει πληροφορίες για σκοπούς συντήρησης. Για παράδειγμα, η επισήμανση ότι η απόδοση μειώθηκε σε ένα λέβητα θα μπορούσε να μας βοηθήσει να διορθώσουμε ένα πρόβλημα πριν ο λέβητας χαλάσει εντελώς [221].

6.1 Case Studies

Arduino weather station data analysis: [224]
Continuous monitoring of wireless network of temperature sensors using MATLAB® and XBee®: [225]
Analyzing IoT sensor data and building predictive algorithms: [226]
Time-series analysis and optimization (bike sharing example): [227]

6.2 Technical Tutorials

ARM mbed and IBM Bluemix: [228]
Raspberry Pi and ThingWorx: [229]
ARM based boards and VIPER: [230]
Sensor networks and Waspmote: [231]
Analytics with Intel Internet of Things: [232]

References

(1) http://osarena.net/internet-things-diadiktyo-ton-pragmaton-ti-einai-ayto
(2) http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/5788/INTERNET%20OF%20THINGS.%CE%A0%CE%A9%CE%A3%20%CE%98%CE%91%20%CE%95%CE%A0%CE%97%CE%A1%CE%95%CE%91%CE%A3%CE%95%CE%99%20%CE%A4%CE%97%CE%9D%20%CE%9A%CE%9F%CE%99%CE%9D%CE%A9%CE%9D%CE%99%CE%91%20%CE%A3%CE%A4%CE%9F%20%CE%9C%CE%95%CE%9B%CE%9B%CE%9F%CE%9D..pdf?sequence=1&isAllowed=y
(3) https://www.sas.com/el_gr/insights/big-data/internet-of-things.html
(4) https://www.newsbeast.gr/weekend/arthro/3239249/to-technologiko-mellon-tis-anthropotitas-pou-sintelite-idi-sti-silicon-valley
(5) http://biztech.gr/iot-internet-tou-uellontos-uas/
(6) http://ru6.cti.gr/ru6/system/files/bouras_site/ergasies/diplwmatikes/ntarzanos_5g.pdf?language=el

(7) https://into.aalto.fi/download/attachments/12324178/Huang_Fuguo_thesis_2.pdf
(8) https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1324973/theFile
(9) http://nefeli.lib.teicrete.gr/browse/stef/epp/2014/KontakiEleftheria,PapadogiannisNikolaos/attached-document-1415604998-766153-1169/KontakiEleftheria_PapadogiannisNikolaos2014.pdf
(10) https://www.teilar.gr/dbData/ProfAnn/profann-e0af756b.pdf
(11) http://image.sciencenet.cn/olddata/kexue.com.cn/bbs/upload/12615WSN-2007.pdf
(12) http://www.electronicdesign.com/what-s-difference-between/what-s-difference-between-ieee-802154-and-zigbee-wireless
(13) http://nemertes.lis.upatras.gr/jspui/bitstream/10889/9048/6/Zappis%28ele%29.pdf
(14) http://www.sase.com.ar/2011/files/2010/11/SASE2011-Protocolos_para_Redes_de_Sensores_Inalambricos.pdf
(15) http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/4771/%CE%91%CE%A3%CE%A5%CE%A1%CE%9C%CE%91%CE%A4%CE%91%20%CE%94%CE%99%CE%9A%CE%A4%CE%A5%CE%91%20%CE%91%CE%99%CE%A3%CE%98%CE%97%CE%A4%CE%97%CE%A1%CE%A9%CE%9D-%CE%93%CE%99%CE%A9%CE%A1%CE%93%CE%9F%CE%A3%20%CE%93%CE%9F%CE%A5%CE%A3%CE%97%CE%A3.pdf?sequence=1
(16) http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/2388/CIED%20%CE%9B%CE%91%CE%93%CE%9A%CE%A9%CE%9D%CE%97.pdf?sequence=1&isAllowed=y
(17) http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/3617/Paulou.pdf?sequence=2
(18) https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php
(19) https://www.postscapes.com/internet-of-things-protocols/
(20)
(21) https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/#datalink
(22) http://www.rfidjournal.com/articles/view?4986
(23) https://www.digitallife.gr/how-quantum-computers-work-68054
(24) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5492403/
(25) http://www.youriothings.com/?page_id=1343
(26) http://repfiles.kallipos.gr/html_books/1285/bookES.html
(27) http://nemertes.lis.upatras.gr/jspui/bitstream/10889/3907/1/Diplomatiki%20Ergasia%20George%20Stefanopoulos.pdf
(28) http://www.ics.uci.edu/~dsm/ics280sensor/readings/networks/routing-survey.pdf
(29) http://nemertes.lis.upatras.gr/jspui/bitstream/10889/4604/1/%CE%91%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%B1%20%CE%94%CE%AF%CE%BA%CF%84%CF%85%CE%B1%20%CE%91%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CF%89%CE%BD.pdf
(30) http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/5152/CIED%20%20%20%20%20%20%20%20%20%20%20%20-%20%20%20%20%20%20%20%20%20%20%20%20%20.pdf?sequence=1
(31) https://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/#6cec6cef10de
(32) http://internetofthingsrecruiting.com/the-history-of-iot/
(33) https://www.thestreet.com/story/13856297/1/a-brief-history-of-the-internet-of-things.html
(34) http://www.baselinemag.com/networking/slideshows/a-brief-history-of-the-internet-of-things.html
(35) http://mqtt.ximxim.com/brief-history-internet-things/
(36) https://en.wikibooks.org/wiki/A_Bit_History_of_Internet/Chapter_8_:_Internet-of-Things
(37) http://www.technologyguide.com/feature/internet-of-things/

(38) https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/
(39) http://www.smart-systems.gr/%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%BF-%CF%83%CF%80%CE%AF%CF%84%CE%B9
(40) http://www.vodafone.gr/portal/client/cms/viewCmsPage.action?pageId=12036
(41) https://www.pcsteps.gr/213103-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-internet-of-things-iot-smart-home/
(42) http://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT
(43) https://www.pcsteps.gr/213103-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-internet-of-things-iot-smart-home/
(44) https://www.myota.gr/index.php/k2-tags/2013-02-13-13-23-56/140-2013-03-19-04-55-08/11393-big-data
(45) http://ir.lib.uth.gr/bitstream/handle/11615/46118/14080.pdf?sequence=1
(46) https://www.fingent.com/blog/role-of-data-analytics-in-internet-of-things-iot
(47) https://www.intel.com/content/www/us/en/big-data/unstructured-data-analytics-paper.html
(48) http://hypatia.teiath.gr/xmlui/bitstream/handle/11400/20185/lb_04174_thanos_thesis.pdf?sequence=1
(49) https://el.wikipedia.org/wiki/Packet_Tracer
(50) https://www.packettracernetwork.com/internet-of-things/pt7-iot-devices-configuration.html
(51) https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CE%B1%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CF%89%CE%BD
(52) http://teachers.teicm.gr/kalomiros/Mtptx/e-books/Embedded_PIC_new.pdf
(53) https://en.wikipedia.org/wiki/Sensor_node
(54) http://www.efxkits.com/blog/various-types-of-sensors-applications/
(55) https://dzone.com/articles/iot-systems-sensors-and-actuators
(56) http://www.ieec.uned.es/investigacion/Dipseil/PAC/archivos/More%20on%20Transducers%20Sensors%20and%20Actuators.pdf
(57) https://learniot.wordpress.com/2016/03/29/actuators-in-iot/
(58) https://eclass.uoa.gr/modules/document/file.php/CHEM217/%CE%A0%CE%BF%CE%BB%CF%85%CE%BC%CE%B5%CF%81%CE%B9%CE%BA%CE%BF%CE%AF%20%CE%91%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CE%B5%CF%82.pdf
(59) http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/2378/CIED%20%CE%BA%CE%BF%CE%BD%CE%B4%CF%85%CE%BB%CE%BF%CF%80%CE%BF%CF%85%CE%BB%CE%BF%CF%85.pdf?sequence=1&isAllowed=y
(60) https://dspace.lib.uom.gr/bitstream/2159/15563/3/SpendasApostolosMsc2012.pdf
(61) http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/2687/Bravos.pdf
(62) http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/12700/1/DT2015-0051.pdf
(63) White Paper EnOcean: Wireless sensor solution for home & building automation- the successful standard uses energy harvesting, white paper, EnOcean Alliance, August 2007
(64) EnOcean, “Specification V 1.0: EnOcean Radio Protocol”, EnOcean , Germany, February 2011
(65) https://en.wikipedia.org/wiki/EnOcean
(66) JP Norair, ”Benefits of DASH7 technology”, December 2009 http://www.dash7.org/DASH7%20Technology%202009-2011%20Seoul%20Briefing.pdf
(67) https://en.wikipedia.org/wiki/DASH7

(68) J. K. Stevens, “An Introduction to RuBee (IEEE P1902.1) and Its Use in Real-Time Visibility Networks” , IEEE RFID, 2007
(69) http://en.wikipedia.org/wiki/RuBee
(70) www.isa.org/isa100 International Society of Automation, “ISA-100.11a-2009, wireless systems for industrial automation: process control and related applications”
(71) International Society of Automation , “The ISA100 Standards Overview & Status”, 2008 www.isa.org/isa100
(72) International Society of Automation Std, ISA100.11a: An Update on the First Wireless Standard Emerging from the Industry for the Industry, ISA 2007 www.isa.org/isa100
(73) http://en.wikipedia.org/wiki/ISA100.11a
(74) International Society of Automation , “The ISA100 Standards Overview & Status”, 2008 www.isa.org/isa100
(75) D. E. Culler, J. Hui, “6LoWPAN Tutorial IP on IEEE 802.15.4 Low-Power Wireless Networks”, ArchRock http://robotics.eecs.berkeley.edu/~pister/290Q/Handouts/6LoWPAN-tutorial.pdf
(76) https://en.wikipedia.org/wiki/6LoWPAN
(77) L. Hester, Y. Huang, O. Andric, A. Allen, P.Chen, “neuRFon Netform: A Self-Organizing Wireless Sensor Network”, Motorola Labs, USA http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.5010
(78) http://en.wikipedia.org/wiki/NeuRFon
(79) Tjensvold, J.M. (2007), “Comparison of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards”
(80) Ergen, S.C. (2004), “ZigBee/IEE 802.15.4 Summary”
(81) S. Farahani,ZigBee Wireless Networks and Transceivers, Elsevier, 2008
(82) http://en.wikipedia.org/wiki/IEEE_802.15.4
(83) φωτο zigbee Vanzago Laura, Overviewon802.15.4/ZigBee
(84) ZigBee Alliance,“Zigbee Specification: ZigBee Document 053474r06”
(85) ZigBee Alliance,“Zigbee Specification: ZigBee Document 053474r07”
(86) ZigBee Alliance,“Zigbee Specification: ZigBee Document 053474r13”
(87) ZigBee Alliance,“Zigbee Specification: ZigBee Document 053474r14”
(88) ZigBee Alliance,“Zigbee Specification: ZigBee Document 053474r15”
(89) ZigBee Alliance,“Zigbee Specification: ZigBee Document 053474r16”
(90) http://en.wikipedia.org/wiki/ZigBee
(91) http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf
(92) http://www.glynstore.com/content/docs/bluegiga/BLE_getting_started.pdf
(93) https://www.inf.ethz.ch/personal/hvogt/proj/btmp3/Datasheets/Bluetooth_11_Specifications_Book.pdf
(94) https://en.wikipedia.org/wiki/Bluetooth_Low_Energy
(95) http://educypedia.karadimov.info/library/DOC1991.PDF
(96) http://www.glynstore.com/content/docs/bluegiga/BLE_getting_started.
(97) http://chapters.comsoc.org/vancouver/BTLER3.pdf
(98) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.3779&rep=rep1&type=pdf
(99) Ammari,H. M., Sahin, D. (2014), “The Art of Wireless Sensor NetworksVolume 1: Fundamentals”, Volume. 1: Fundamentals, New York City: Springer.
(100) Song, H., Song, J., Zhu, X., Mok, A.K., Chen, D., Nixon, M., Pratt, W., Giondhalekar, V. (2009), “Wi-Htest: compliance test suite for Diagmosing Devices in Real-Time WirelessHART Network”, RTAS 2009, in 15thIEEE, Real-Time and Embedded Technology and Applications Symposium, pp. 327-336, 13-16.

(101) Song, J., Han, S., Mok, A., Chen, D., Lucas, M., Nixon, M. and Pratt, W. (2008), "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control", in IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS 2008, pp. 377-386, 22-24.
(102) Lennvall, T., Svensson, S., and Hekland, F. (2008), "A Comparison of WirelessHART and ZigBee for Industrial Applications", IEEE International Workshop on, pp. 85-88.
(103) Radmand, P., Talevski, A., Petersen S. (2010), "Comparison of Industrial WSN Standards"4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST).
(104) Nixon, M. (2012), "A Comparison of WirelessHART and ISA100.11a"
(105) Γ. Πάγκαλος, Ι. Μαυρίδης, Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων
(106) Δημήτριος Κουτσουβέλας, Ηλίας Κωστούδης, "Ασφάλεια σε δίκτυα ad hoc και δίκτυα αισθητήρων", Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, 2008
(107) D. Djenouri, L. Khelladi, "A Survey of security issues in mobile ad hoc and sensor networks", IEEE Communication Surveys, 2005 https://www.researchgate.net/publication/3454630_A_survey_of_security_issues_in_mobile_ad_hoc_and_sensor_networks
(108) W. Stallings, "Cryptography and Network Security Principles and Practices",3rd edition, Pearson Education Inc, 2003 http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf
(109) A. Perrig, R. Szewczyk, V. Wen, D. culler, J. Tygar, "SPINS: security protocols for sensor networks" Proc. 7th Annual ACM International Conference on Mobile Computing and Networks (Mobicom 2001) https://people.eecs.berkeley.edu/~tygar/papers/SPINS/SPINS_mobicom.pdf
(110) F. Hu, N. K. Sharma, "Security considerations in ad hoc sensor networks", Computer Science (Elsevier) http://www.cs.mun.ca/~yzchen/papers/papers/security_coordination/security_consi_manet_hu_2005.pdf
(111) S. Zhu, S. Setia, S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", Proc. 10th ACM conference on computer communications security, Washington, DC, USA 2003 http://www.cse.psu.edu/~sxz16/papers/leap.pdf
(112) Z. Yan, "Security in ad hoc networks", Networking Laboratory, Helsinki University of Technology
(113) W. Seah, Y. K. Tan, "Sustainable Wireless Sensor Networks", InTech, 2010 https://www.intechopen.com/books/sustainable-wireless-sensor-networks
(114) D. W. Carman, P. S. Krus, B. J. Matt, "Constraints and approaches for distributed sensor network security", tech. report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, USA , 2000 http://www.csee.umbc.edu/courses/graduate/CMSC691A/Spring04/papers/nailabs_report_00-010_final.pdf
(115) http://edurenew.blogspot.com/2017/03/application-of-wireless-sensor-network.html
(116) https://www.researchgate.net/publication/230660610_Modeling_the_Behavior_of_an_Electronically_Switchable_Directional_Antenna_for_Wireless_Sensor_Networks
(117) I. F. Akyilditz, W. Su, Y. Sankarasubramamian, E. Cayirci, "Wireless Sensor Networks: A survey", Computer Networks, 2002
(118) J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey", Computer Networks, 2008
(119) K. Sohraby, D. Minoli, T. Znati, Wireless sensor networks: Technology, Protocols, and Applications, Wiley, 2007
(120) I. F. Akyildiz, M. C. Vuran, Wireless Sensor Networks, Willey, 2010

(121) K. Martinez, J.K. Hart, R. Ong, “Environmental Sensor Networks”, IEEE Computer, Manuscript id, 2004 http://eprints.soton.ac.uk/259997/1/martinez11.pdf
(122) Mainwaring, D. Culler, J. Polastre, R. Szewczyk, J. Anderson, “Wireless sensor networks for habitat monitoring”, Proc. 1st ACM internationalWorkshop on Wireless Sensor Networks and Applications (WSNA '02), ACM Press, New York, September 2002 http://doi.acm.org/10.1145/570738.570751 author's site 2002
(123) G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees, M. Welsh, “Monitoring Volcanic Eruptions with a Wireless Sensor Network,” Proc. 2nd European Workshop Wireless Sensor Networks (EWSN 05), IEEE Press, 2005
(124) D. Culler, D. Estrin, M. Srivastava, “Overview of Sensor Networks”, IEEE Computer, Vol. 37, No.8, August 2004 http://compilers.cs.ucla.edu/emsoft05/CullerEstrinSrivastava04.pdf
(125) P. Zhang, C. Sadler, S. Lyon, M. Martonosi, “Hardware design experiences in ZebraNet”, Proc. ACM SenSys’04, Baltimore, USA, November 2004
(126) https://www.sciencedirect.com/science/article/pii/S1084804515002702
(127) M. Hefeeda, S. Fraser ,“Forest Fire Modeling and Early Detection using Wireless Sensor Networks”, University Canada http://www.cs.sfu.ca/~mhefeeda/Papers/ahswn09a.pdf
(128) R. G. Lee, K. C. Chen, S. S. Chiang, C. C. Lai, H. S. Liu, M. S. Wei, “A Backup Routing with Wireless Sensor Network for Bridge Monitoring System”, Proc. 4th Annual Communication Networks and Services Research Conference (CNSR’06), Computer Networks, 2006
(129) https://en.wikipedia.org/wiki/Wireless_sensor_network
(130) https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=2ahUKEwj17qDZidLdAhWFMewKHcQPBcIQjhx6BAgBEAM&url=http%3A%2F%2Fthinkspace.csu.edu.au%2Fwirelesssensorsnetworking11567963%2F2016%2F06%2F03%2Fwhat-is-wsn-and-how-to-use-wsn-for-smart-home%2F&psig=AOvVaw3US1AbUngOMot75EimcyFb&ust=1537824722749409
(131) L. Krishnamurthy, R. Adler, P. Buonadonna, J. Chhabra, M. Flanigan, N. Kushalnagar, L. Nachman, M. Yarvis, “Design and Deployment of Industrial Sensor Networks: Experiences from a Semiconductor Plant and the North Sea”, Proc. 3rd International Conference on Embedded Networked Sensor Systems (SenSys '05), November 2005 https://lasr.cs.ucla.edu/yarvis/Papers/f194-krishnamurthy_distro.pdf
(132) M. Ilyas, I. Mahgoub, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, 2004
(133) E. Shih, V. Bychkovsky, D. Curtis, J. Guttag, “Demo Abstract: Continuous Medical Monitoring Using Wireless Microsensors”, Proc. 2nd International Conference on Embedded Networked Sensor Systems(SenSys’04), Baltimore, Maryland, November 2004 http://ddmg.csail.mit.edu/publications/medical-monitoring-abstract-sensys2004.pdf
(134) T. V. Ngoc, “Medical Applications of Wireless Networks: A survey paper written under guidance of Prof. Raj Jain” https://ecse.monash.edu/staff/mehmety/Jofmedical2007.pdf
(135) https://www.cse.wustl.edu/~jain/cse574-08/ftp/medical/
(136) Gartner, "Gartner's 2014 hype cycle for emerging technologies maps the journey to digital business,", August 2014, http://www.gartner.com/newsroom/id/2819918
(137) Internet of Things Protocols and Standards https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/#datalink
(138) IEEE 802.15.4-2011 IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," 314 pp., Sept. 5 2011, http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf

(139) Z-Wave, "Z-Wave Protocol Overview," v. 4, May 2007, https://wiki.ase.tut.fi/courseWiki/images/9/94/SDS10243_2_Z_Wave_Protocol_Overview.pdf
(140) J. Decuir, "Bluetooth 4.0: Low Energy", Presentation slides, 2010 http://chapters.comsoc.org/vancouver/BTLER3.pdf
(141) C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology," Sensors, vol. 12, no. 9, pp. 11734-11753, 2012, http://www.mdpi.com/1424-8220/12/9/11734
(142) Galeev M., Catching the Z-Wave, Electronic Engineering Times India, October 2006. http://www.drdobbs.com/embedded-systems/catching-the-z-wave/193104353
(143) z-wave protocol stack | z-wave protocol layer basics http://www.rfwireless-world.com/Tutorials/z-wave-protocol-stack.html
(144) https://www.silabs.com/documents/public/user-guides/ug103-11-appdevfundamentals-thread.pdf
(145) https://en.wikipedia.org/wiki/Thread_(network_protocol)
(146) https://tools.ietf.org/html/rfc4291
(147) Neighbor Discovery Optimi-zation for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) https://tools.ietf.org/html/rfc6775
(148) Τοπολογία δικτύου https://el.wikipedia.org/wiki/%CE%A4%CE%BF%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1_%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85
(149) Gartner, Newsroom, Gartner identifies the top 10 IoT technologies for 2017 and 2018 https://www.gartner.com/newsroom/id/3221818
(150) http://ir.lib.uth.gr/bitstream/handle/11615/45970/15460.pdf?sequence=1
(151) https://www.cse.wustl.edu/~jain/cse574-14/ftp/coap/#sec4-1 Constrained Application Protocol for Internet of Things, Xi Chen chen857 (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain)
(152) Kothmayr T., Schimitt C., Wen Hu, Bruning M., (2012) " A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-Way Authentication ", Technische Universitat , Munchen, Germany
(153) https://jesusalonsozarate.files.wordpress.com/2015/01/2015-transaction-on-iot-and-cloud-computing.pdf V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015
(154) http://www.ietf.org/rfc/rfc7252.txt
(155) https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/#datalink
(156) https://cy.ipc2u.com/articles/articles-and-reviews/ti-einai-to-mqtt-kai-giati-to-chreiazomaste-sto-iiot/
(157) Dinesh Thangavel, Xiaoping Ma, Alvin Valera, Hwee-Xian Tan, Colin Keng-Yan Tan, Performance Evaluation of MQTT and CoAP via a Common Middleware, IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 21-24 April 2014, pp. 1-6.
(158) https://www.cyberinsurancegreece.com/news/internet-of-things-prokliseis-stratigiki-asfaleias/
(159) https://www.cyberinsurancegreece.com/nomothesia/iot/
(160) hellanicus.lib.aegean.gr/bitstream/handle/11610/18346/διπλωματική μεταπτυχιακού.pdf?sequence=2&isAllowed=y
(161) http://www.futuremobility.gr/connectivity/why-connected-vehicles-are-important
(162) https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
(163) https://www.apple.com/ios/home/accessories/
(164) http://conta.uom.gr/conta/ekpaideysh/seminaria/M_Telecommunications/30main.htm
(165) Κ.Χ Κυριαζής&Ε.Γ Παπαδάκης Μάρτιος 2009

(166) http://www.dga.gr/web/publications/files/networks.pdf
(167) http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/4917/713.pdf?sequence=1
(168) https://stevessmarthomeguide.com/build-home-network/#setup
(169) https://www.theseus.fi/bitstream/handle/10024/62819/Zheng_Zeya.pdf?sequence=1
(170) http://enersolv.ca/common-components-hvac-systems/
(171) https://vasco.eu/en-gb/blog/heating-general/what-ideal-room-temperature-your-living-room-bathroom-and-bedroom
(172) https://lightwaverf.com/collections/control-smart-series/products/link-plus
(173) https://www.ecobee.com/ecobee3-lite/
(174) http://www.virusbeta.net/Cisco/CCNA1_cap.10.pdf
(175) https://el.wikipedia.org/wiki/%CE%94%CE%BF%CE%BC%CE%B7%CE%BC%CE%AD%CE%BD%CE%B7_%CE%BA%CE%B1%CE%BB%CF%89%CE%B4%CE%AF%CF%89%CF%83%CE%B7
(176) https://el.wikipedia.org/wiki/%CE%9F%CE%BC%CE%BF%CE%B1%CE%BE%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C_%CE%BA%CE%B1%CE%BB%CF%8E%CE%B4%CE%B9%CE%BF
(177) https://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/Antennas_EMR/health/BaseStationRdt/BaseStation/
(178) https://searchnetworking.techtarget.com/definition/coaxial-cable-illustrated
(179) https://community.fs.com/blog/fiberstore-cables-how-to-identify-the-color-code-of-fiber-optic-cable.html
(180) https://www.projectorscreen.com/store/p/129165-QVS-CABSSV35FC-10ft-SmartSerial-to-DCE-V-35-Serial-Cisco-Router-Cable.html
(181) https://el.wikipedia.org/wiki/Ethernet
(182) https://www.amazon.co.uk/Belkin-Cat5e-Moulded-Crossover-Cable/dp/B0001GYOGO
(183) https://devilprinters.co.uk/home/5776-18m-network-ethernet-cable-straight-through.html
(184) http://opticalfiberalsa.over-blog.com/2016/09/how-to-configure-rj45-pinout.html
(185) https://www.slideshare.net/vmantza/t-40561328
(186) https://juniperpublishers.com/etoaj/pdf/ETOAJ.MS.ID.555593.pdf
(187) http://ru6.cti.gr/ru6/system/files/bouras_site/ergasies_foithtwn/algo_dromologisis_stogiannou.pdf
(188) http://www.ece.iastate.edu/~kamal/Docs/kk04.pdf
(189) https://ijcsmc.com/docs/papers/June2014/V3I6201499a40.pdf
(190) http://ikee.lib.auth.gr/record/290395/files/text.pdf
(191) Heinzelman, W., Kulik, J., & Balakrishnan, H. (1999, August). Adaptive protocols for information dissemination in wireless sensor networks. Presented during the proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99), Seattle, WA.
(192) Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000, August). Directed diffusion: A scalable and robust communication paradigm for sensor networks. Presented during the proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA.
(193) Braginsky, D., & Estrin, D. (2002, October). Rumor Routing Algorithm for Sensor Networks. Presented during the proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA.
(194) Schurgers, C., & Srivastava, M.B. (2001). Energy efficient routing in wireless sensor networks. Presented during the MILCOM proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA.
(195) Chu, M., Haussecker, H., & Zhao, F. (2002). Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks. The International Journal of High-Performance Computing Applications, 16 (3).

(196) Heinzelman, W., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy efficient communication protocol for wireless sensor networks. Presented during the proceedings of the Hawaii International Conference on System Sciences, Hawaii.

(197) Lindsey, S., & Raghavendra, C.S. (2002, March). PEGASIS: Power Efficient Gathering in Sensor Information Systems. Presented during the proceedings of the IEEE Aerospace Conference, Big Sky, Montana.

(198) Manjeshwar, A., & Agrawal, D.P. (2001, April). TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks. Presented during the proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA.

(199) Manjeshwar, A., & Agrawal, D.P. (2002, April). APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks. Presented during the proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, Ft. Lauderdale, FL.

(200) Rodoplu, V., & Ming, T.H. (1999). Minimum energy mobile wireless networks. IEEE Journal of Selected Areas in Communications, 17(8), 1333-1344.

(201) Xu, Y., Heidemann, J., & Estrin, D. (2001, July). Geography informed energy conservation for ad hoc routing. Presented during the proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'01), Rome, Italy.

(202) Yu, Y., Estrin D., & Govindan R. (2001). Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks. UCLA Computer Science Department Technical Report, UCLA-CSD-TR-01-0023.

(203) Zorzi, M., & Rao, R. (2003). Geographic Random Forwarding (GeRaF) for Ad Hoc and sensor networks: Energy and Latency Performance, IEEE Transactions on Mobile Computing, 2 (4).

(204) Zorzi, M., & Rao, R. (2003). Geographic Random Forwarding (GeRaF) for Ad Hoc and sensor networks: Multihop performance. IEEE Transactions on Mobile Computing, 2 (4).

(205) Chang, J.H., & Tassiulas, L. (2000, March). Maximum Lifetime Routing in Wireless Sensor Networks. Presented during the proceedings of the Advanced Telecommunications and Information Distribution Research Program (ATIRP'2000), College Park, MD

(206) Kalpakis, K., Dasgupta, K., & Namjoshi, P. (2002, August). Maximum lifetime data gathering and aggregation in wireless sensor networks. Presented during the proceedings of IEEE International Conference on Networking (NETWORKS '02), Atlanta, GA.

(207) Chu, M., Haussecker, H., & Zhao, F. (2002). Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks. The International Journal of High Performance Computing Applications, 16 (3).

(208) Sohrabi, K., Gao, J., Ailawadhi, V., & Pottie, G.J. (2000). Protocols for self-organization of a wireless sensor network. IEEE Personal Communications,7(5), 16-27.

(209) He, T., Stankovic, J., Lu, C., & Abdelzaher, T. (2003, May). SPEED: A stateless protocol for real time communication in sensor networks. Presented during the proceedings of International Conference on Distributed Computing Systems, Providence, RI.

(210) Chen, B., Jamieson, K., Balakrishnan, H., & Morris, R. (2001, July). SPAN: An Energy Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks. Presented during the proceedings of the Seventh annual international Conference on Mobile Computing and Networking, Rome, Italy

(211) Xu, Y., Heidemann, J., & Estrin, D. (2001, July). Geography informed energy conservation for ad hoc routing. Presented during the proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'01), Rome, Italy.

(212) Schurgers, C., Tsiatsis, V., Ganeriwal, S., & Srivastava, M. (2002). Optimizing sensor networks in the Energy-Latency-Density design space. IEEE Transactionson Mobile Computing,1 (1), 70-80.
(213) S. Nikolidakis, D. Kandris, D. Vergados, C. Douligeris, Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering. *Algorithms*, 2013, Vol. 6, Issue 1, pp. 29-42
(214) https://techblog.gr/internet/tech-how-to-7-steps-for-a-safer-wireless-network-02343/
(215) https://www.apple.com/shop/accessories/all-accessories/homekit
(216) https://www.apple.com/airplay/
(217) https://support.apple.com/en-us/HT204893
(218) https://support.apple.com/en-us/HT204085
(219) https://www.gartner.com/en/newsroom/press-releases/2017-03-06-gartner-survey-shows-connected-home-solutions-adoption-remains-limited-to-early-adopters
(220) https://www.ics.uci.edu/~dsm/ics280sensor/readings/networks/routing-survey.pdf
(221) https://www.trustedreviews.com/opinion/4-ways-smart-home-needs-improve-2019-3638510
(222) file:///C:/Program%20Files/Cisco%20Packet%20Tracer%207.2/help/default/index.htm
(223) https://www.tomsguide.com/us/pictures-story/1106-best-homekit-compatible-devices.html#s2
(224) http://makerzone.mathworks.com/resources/arduino/weather-station-data-analysis/
(225) http://uk.mathworks.com/matlabcentral/fileexchange/47757-continuous-monitoring-of-wireless-network-of-temperature-sensors-using-matlab%C2%AE-and-xbee%C2%AE
(226) http://uk.mathworks.com/solutions/internet-of-things/analyzing-iot-sensor-data-and-building-predictive-algorithms.html
(227) https://www.knime.org/files/internet_of_things_with_knime_final1.pdf
(228) https://developer.ibm.com/recipes/tutorials/arm-mbed-iot-starter-kit-part-1/
(229) http://www.thingworx.com/Academics/Example-IoT-Projects/Weather-Applications-With-Raspberry-Pi
(230) http://doc.viperize.it/0.2.0.0009/supported_boards.html
(231) http://www.libelium.com/development/waspmote/documentation/wireless-sensor-networks-with-waspmote-meshlium/
(232) https://software.intel.com/en-us/articles/the-internet-of-things-analytics-using-the-intel-iot-analytics-website-for-data-mining